AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 106–186

ANSWERING THE CALL FOR HELP: THE IMPACT OF Y2K ON 911 AND LAW ENFORCEMENT?

HEARING

BEFORE THE

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

THE IMPACT OF Y2K ON TWO SPECIFIC AREAS OF EMERGENCY PREPAREDNESS, 911 SYSTEMS AND LOCAL LAW ENFORCEMENT

APRIL 29, 1999

Printed for the use of the Committee

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

56-951 CC WASHINGTON : 1999

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

SPECIAL COMMITTEE ON THE
YEAR 2000 TECHNOLOGY PROBLEM

[Created by S. Res. 208, 105th Cong., 2d Sess. (1998)]

ROBERT F. BENNETT, Utah, *Chairman*

JON KYL, Arizona
GORDON SMITH, Oregon
SUSAN M. COLLINS, Maine
TED STEVENS, Alaska, *Ex Officio*

CHRISTOPHER J. DODD, Connecticut,
Vice Chairman
JOHN EDWARDS, North Carolina
DANIEL PATRICK MOYNIHAN, New York
ROBERT C. BYRD, West Virginia, *Ex Officio*

ROBERT CRESANTI, *Staff Director*
T.M. (WILKE) GREEN, *Minority Staff Director*

CONTENTS

STATEMENT BY COMMITTEE MEMBERS

CHRONOLOGICAL ORDER OF WITNESSES

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

ANSWERING THE CALL FOR HELP: THE IMPACT OF Y2K ON 911 AND LAW ENFORCEMENT

THURSDAY, APRIL 29, 1999

U.S. SENATE,
SPECIAL COMMITTEE ON THE YEAR 2000
TECHNOLOGY PROBLEM,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Robert F. Bennett (chairman of the committee), presiding.

Present: Senator Bennett.

OPENING STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM UTAH, CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Chairman BENNETT. Good morning. The committee will come to order.

Our hearing today marks the second time in 6 months that this committee will address the important topic of Y2K emergency preparedness. On October 2, 1998, we focused on emergency management, and that hearing included testimony from FEMA and the National Guard Association, the National Emergency Managers Association, and the National Governors Association.

Today, we will concentrate on the impact of Y2K on two specific areas of emergency preparedness, 911 systems and local law enforcement. We touched somewhat on those issues during the October 2 hearing, but today, we will address them with a more focused concentration and a heightened sense of concern.

Our concern about these two areas is heightened for two reasons. In a report released last month, the Network Reliability Interoperability Council [NRIC]—we always have to use acronyms in Washington—estimated that only 10 percent of over 7,000 public safety answering points, or PSAP's, where 911 calls are processed, are prepared for Y2K. Let me repeat that. A council that is focusing on this issue says that only 10 percent of the public service answering points where 911 calls are processed were prepared for Y2K.

In an updated report received from the FCC yesterday, this committee was informed that the number might now be as high as 35 percent. Thirty-five percent is a whole lot better than ten, but it is still not comforting enough for us to cancel the hearing. It should be noted that this refers only to the equipment provided to the PSAP's by the telephone companies.

There is still a large amount of equipment and information systems utilized within the PSAP's about which we know very little. An ongoing survey being conducted by the U.S. Fire Administration about overall readiness of 4,300 of these PSAP's indicates that overall readiness is about 17 percent. Survey results indicate some strong concerns about funding on the part of the PSAP's. In other words, they say, well, we think we know what to do, but we do not have any money so we probably are not going to do anything.

Now, put this in perspective. In the United States, there are approximately 300,000 calls for emergency assistance made via the 911 system every day. That does not count the additional 86,000 911 calls made from cellular phones every day. That is over 110 million 911 calls per year. If the problems within the system supporting the answering points that handle these calls, the PSAP's, are not properly addressed, the systems will fail, leading to degradation in the processing of 911 calls.

Let me stress the word degradation does not mean elimination. The 911 calls will still be answered. Someone will still try to handle the emergency. But they will not have available to them all of the computer-assisted support that is there right now, and so the whole system will be degraded and there will obviously be an impact. But it is not a case of either all on or all off.

I would like to announce that Senator Dodd and I are jointly sending a letter to Commissioner Michael Powell, who is with us today and will be on our first panel, from the FCC, and Administrator Carrye Brown of the U.S. Fire Administration asking that they work together to identify those PSAP's that are not yet prepared and those who have not yet responded to the Fire Administration's survey. We have also asked that they provide this information to the appropriate 911 commissions, State Y2K coordinators, and other appropriate regulatory bodies governing those PSAP's.

We hope that this will help the States and local jurisdictions identify potential problems so that help can be provided to those that need it. There may be some people out there who have a problem but do not realize it, even at this late date and after all of the work that has been done to try to publicize this. The supervisor of one PSAP told the committee staff that the radio system in his dispatch center required a $60,000 patch and without this patch they would have been unable to communicate with emergency service units at all.

Now, in regard to local law enforcement, the committee has noted the absence of any overall assessment of the Y2K status of our nation's local law enforcement agencies. At the Federal level, we have captured much information about Federal law enforcement agencies within the Justice Department, Treasury Department, and their subsidiary agencies, FBI, DEA, Customs, ATF, Secret Service, and so on. This information comes to the committee and to the country through the quarterly OMB reports and the work of the inspector general offices of these departments.

The news about these agencies is very good. If not already completely prepared, they are well on their way to being so and we have every confidence they will be able to meet their challenge by January 1, 2000. However, we are concerned about the lack of in-

formation on that segment of law enforcement that our citizens rely on most in their everyday lives, and that is the local law enforcement sector, and this means approximately 17,000 police and sheriff's departments across the country.

We do not want to overstate the problem or needlessly set up public panic. We have no reason to believe that our emergency services are not taking this problem very seriously and working to prepare for Y2K, but there are vulnerable, highly vulnerable areas in the 911 sector as well as the local law enforcement sector and we are concerned about the lack of assessments, the lack of information, that leaves us without any hard data. That is why we are holding the hearing today.

Our lead witness on the first panel will be Mr. Jack Brock, who is Director of Information Management Issues at GAO. Those who follow this committee know that we depend heavily on GAO and Mr. Brock is here often and members of his agency are here often, either in the hearing or working with our staff. Mr. Brock, once again, on behalf of the entire Congress, we thank the GAO for your efforts and your diligence on following through on this. He will explain to us how the 911 systems work and discuss GAO's examination of these systems and its review of the Justice Department and law enforcement working groups' outreach efforts.

He will be joined in the first panel by Commissioner Michael Powell of the Federal Communications Commission. Commissioner Powell is also a familiar face to this committee and to this issue. I have seen him on a number of speaking assignments where I have been, and he has, likewise, been very diligent in following this through. So I think between the two of them, we are going to get a frank and direct response to the challenge that we face. He will explain where the problems in the system may exist and speak to us about what may be the big problem from our point of view, the lack of regulatory authority over PSAP's.

We will proceed with that first panel and start with you, Mr. Brock.

STATEMENT OF JACK L. BROCK, JR., DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, UNITED STATES GENERAL ACCOUNTING OFFICE

Mr. BROCK. Thank you very much, Mr. Chairman. I am pleased to be here today. I am also pleased to be on a panel with Commissioner Powell. I think that Commissioner Powell has done a good job on leading the Communications Sector Work Group, and as a result of his and the Sector Work Group, there is a lot more known about the telecommunications system than we knew a year or so ago.

I would like to briefly summarize my statement. You asked us to comment on a couple of things. First of all, our awareness of the status of 911 systems and State and local law enforcement entities. To that point, unlike Federal agencies, we have no direct audit authority there, so much of our information that we are discussing today has come from surveys and material that are gathered by national associations, that are gathered by the working groups on the President's Conversion Council.

Second, you asked us to comment on the efforts of the President's Council on Year 2000 Conversion and specifically to comment on the outreach efforts of the Department of Justice.

I would like to address 911 first. I am going to give you a very simplified explanation of what happens to a 911 call. There is a chart up behind you, sir. It is also in our statement for people who cannot read it well. But, basically, we are talking about an enhanced 911 calling process. FCC has told us that about 90 percent of the country is covered by 911 services. Of that 90 percent, 95 percent of those services are enhanced, and my description will be a brief overview of an enhanced system.

The first thing, if you notice the telephone up there, the most critical step to making the 911 call is, in fact, picking up the phone and getting a dial tone. If the telephone does not work, then the call stops right there. Fortunately, I think information that has been made available to us by the Communications Working Group, through their efforts working with NRIC and in turn working with the Telco Year 2000 Forum, we have increasing confidence that there will be dial tone.

So we are pretty sure you are going to pick up the phone and you are going to get a dial tone. You are going to go through a switch. That is the next thing. That is going to route you to the appropriate public safety answering point. I will just refer to that from now on as PSAP.

When it goes to the PSAP, it is going to go through their PBX system. If the PBX system does not work, and this is not owned by the telephone company, this is owned by the PSAP, and one of the things that FCC will tell you, that the biggest worry now in communications is not the public switch network, it is the customer premise equipment. They have no control over what you have on your location. That is up to each individual jurisdiction or private party or whatever to make sure that is compliant.

When it goes through there, it is attached with what is called an automatic number identification [ANI], and that comes from the phone company and it goes into a controller, a phone number controller that is maintained by the PSAP. At the same time, it goes back out to the telephone company and at the same time goes to the operator.

The telephone company then supplies from what is called an automatic location index [ALI], the address. So the operator is now getting, over there on the call taker, is now getting from the phone up on their screen the location and the identifier for the phone, and this is only on wire line equipment. If you are making a cell phone call, none of that is coming in.

After the operator takes the call, they typically would verify the information and it would be automatically recorded and time stamped. Then the operator would code the call, enter it into a computer-aided dispatch system, and notify the appropriate response unit. The dispatch system would do such things as——

Chairman BENNETT. And that is not on the chart?

Mr. BROCK. That is not on the chart. That would go outside the chart. But when it goes into the computer-aided dispatch system [CAD], all sorts, depending on the jurisdiction, all sorts of decisions are made for the jurisdiction. What is the most appropriate unit to

respond? Does the address they are responding to have situations that might endanger law enforcement officials or would it contain explosives that might endanger fire officials or any certain amount of information.

If these things do not work, if the location index is not compliant, if the number system does not work, if the CAD system does not work, you essentially revert back to the old basic 911 system, where you get the dial tone, you call in, you reach an operator. This information has to be taken down manually, and then the dispatch is no longer automatic, it is manual and it takes time.

The two PSAP's that we visited locally both said if their systems did not work that there would be a definite degradation of service. There would be an increased waiting time. And depending on the volume of calls, it could affect the safety and well-being of certain individuals.

Chairman BENNETT. Let me see if I understand what you are saying. The phone call would come in off the phone there and go directly to the call taker without any of the other information along the way, is that correct?

Mr. BROCK. Typically, yes. It would be routed through the telephone switch, the tandem switch that is at the telephone office, to the PSAP. Some of the other features, if they did not work, perhaps would not supply the location or the phone number. That would have to be manually input by the operator, and that happens on cell calls right now. That is typically not provided on cell calls, so they are well-equipped to deal with that. The key thing——

Chairman BENNETT. It would just slow everything down.

Mr. BROCK. It would slow things down.

Chairman BENNETT. OK.

Mr. BROCK. The key thing would be the automatic dispatch equipment. That really makes the whole system more efficient in making sure that you send the right unit out there and that that unit has appropriate information on the address they are going to if it is, in fact, in the system.

Chairman BENNETT. OK.

Mr. BROCK. Now, the other thing that we were told when we visited the two PSAP's, that if you have not started remediation of your equipment, it is probably too late, that the lead time for bringing in one of these systems, training your personnel, and getting it up and operational is greater than the amount of time that is available. So if you have not done much now, it is time to go to contingency planning and it may not be possible to bring in the necessary fixes to the system, depending on how extensive they are.

Chairman BENNETT. Do you have any sense of how many people are in that condition, that have not done anything and for whom it is too late?

Mr. BROCK. Well, this gets back to the point of our statement. No. We do not have a good sense of that. While, as I said, we have increasing confidence in what is going on in the public switch network, that confidence resides in the fact that a lot of people are reporting, that appropriate organizations, such as the Telco Year 2000 Forum are doing testing, and that you have information that

remediated systems will work. You still have to complete the remediation.

We have much less information on PSAP's. The information that we have that has been supplied back to FEMA is on a very, very small sample. Only 18 percent, as you mentioned, of the respondents replied back. Sixteen percent said that they were ready now. You had some updated information that was not available to us that indicates that 35 percent say they are ready.

There are a couple of issues here. This is self-reported data. We do not know the extent that testing has been done and we are not sure of the status. So there is a lack of awareness, a general lack of awareness of where these PSAP's stand.

FEMA is now working to update their survey. They are going to be doing telephone surveys now. They are going to try to get a much more vigorous response so the assessment data will be more complete.

Chairman BENNETT. When it comes in, it will all be self-reported?

Mr. BROCK. It will all be self-reported. We do know from the two local jurisdictions that we went to that they have done extensive tests. For example, on April 14, Fairfax County did do a complete test of their system, of the equipment that they own, and they have been working over a year and a half to remedy the situation, and it worked. They had a successful test.

Chairman BENNETT. Have you done any examination in the District?

Mr. BROCK. We are doing District Y2K work. As I reported a couple of months ago, the District is far behind. We did not specifically look at their 911 system, but all of their systems are far behind and they are not scheduled to begin testing until late in the year on most of their key systems.

We have evidence here in the local community that Montgomery County, Fairfax County, Arlington, places like that have made good progress. The District's progress has not been as good, generally.

In terms of outreach, we found, because of the interaction at the local level with the PSAP's that FEMA has some responsibility for, in its outreach committee, the emergency services outreach, and then, of course, the Communications Working Group that SEC and GSA co-chair, that there has been a fair amount of outreach. FEMA has had a number of events all across the country. They have been targeting PSAP's. Associations that are connected with PSAP, as well as the telephone companies, have also been very active in contacting PSAP's to discuss their Y2K readiness. So there has been a fair amount of outreach. That outreach has not always generated the kind of information that would allow us today to say, this is the status. We do not know.

And again, echoing your remarks, Mr. Chairman, I do not want to alarm people. We believe that, at a minimum, basic 911 service will work, but there could be a degradation of service if remediation action is not directed.

You also asked us to look at State and local law enforcement agencies, and we have almost no information there. I would like to read a quote from the first sector assessment of the President's Conversion Council, where they reported that, "Based on informal

assessment information, there is a high level of awareness of the problem among non-Federal police/law enforcement entities. State police/law enforcement entities and departments in larger metropolitan areas are making good progress. However, most departments at the county and municipality level lack the sophistication to assess the Y2K readiness of their service providers. These departments do not have their own dedicated IT resources. They do not have money or professional staffing and are instead dependent on the IT departments of the county, city, or municipality of which they are a part. Dedicated radio communications and dispatch systems are a concern for all public law enforcement organizations and the working group is encouraging departments to focus on contingency planning in this area." So the assessments are basically informal and there is not a lot of direct information on the status of law enforcement entities, and there are about 17,000 of these across the country. Of course, some States, some jurisdictions, have done very detailed assessments, so there is information in pockets, but there is not a good source of national information.

In fact, because of the importance of 911 systems and law enforcement systems throughout the country, this was exactly one of the reasons that the Y2K Conversion Council was created, that in areas that were of immense national concern but where there may not be direct Federal intervention, it was thought that the Conversion Council, in conjunction with associations, civic groups, et cetera, could work together and collaboratively to determine the status of various key sectors and then recommend remedial action.

We recommended last April that the Conversion Council begin to do assessments to determine the status of their relevant sectors. In October, the Council did send out guidance to all of the working groups to develop such information. Information was developed on PSAP's. To date, no information has been developed by the working group, except informal stuff, on law enforcement. We understand last week that the law enforcement sector has agreed to do a survey in conjunction with FEMA to develop some initial assessment information, and this should be useful once that is done.

One of the key points, though, I would like to make, Mr. Chairman, in closing, that just gathering assessment information is not enough. You have to do something with it. So, for example, depending on the status of that information and what it indicates, you have some options ranging from wringing your hands and saying, "We are in a bad situation," to taking some decisive action, and I think that is what is going to be incumbent upon the various sectors as this information rolls in.

Again, depending on what the information says, you are going to need to be a lot more specific in terms of what sort of action you can take that will be effective, because the types of services that we are talking about at the local level are really the services that are going to impact citizens most often on January 1.

I mean, a lot of the Federal systems that we are looking at are critically important to the nation, but midnight Friday night and into Saturday morning, those are not going to be the systems that affect you and I in our house. I am going to turn on my light switch, I am going to pick up my phone, I am going to see if my power is on, my water turns on. These are the kinds of things that

we are going to be looking at, and if these services do not work, there will be an impact at the local community level.

Again, not to be an alarmist, we do not know the status, and that is the concern. If the status is known, then there can be decisions made on the appropriate action that should be taken.

That concludes my statement, Mr. Chairman.

Chairman BENNETT. Thank you very much. I appreciate it and appreciate your patience in allowing me to question you back and forth and thus interrupt you. I think that helps us understand the scope of the problem.

[The prepared statement of Mr. Brock can be found in the appendix.]

Chairman BENNETT. Commissioner Powell.

STATEMENT OF MICHAEL K. POWELL, COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

Mr. POWELL. Thank you, Senator Bennett. As always, it is a pleasure to be here. If I could just take a moment to echo the sentiments that you expressed in terms of the strong working relationship we have had with the committee, we have enjoyed it and I think we have made some substantial progress.

I would also like to thank GAO, who have worked increasingly with us on this pressing national problem, particularly with respect to public safety, which, of course, in many cases Y2K failings or shortcomings will range from humorous to bothersome. In this case, it could cost lives, and so that places an exclamation mark on the urgency of these efforts.

I also wanted to state unequivocally we would be more than happy to accept your suggestion and invitation to work with the Fire Administration to advance our outreach efforts and we will start on that immediately as an extension of things we are doing. I think it is a nice complement to something we have been trying to emphasize already, which is we have been imploring State regulatory commissions, particularly through the National Association of Regulatory Utility Commissioners, to make PSAP's and public safety a central component of their Y2K efforts because of their localized responsibilities and their ability to more easily canvas. They have regularly committed to me that they would be willing to do that and I think that we can use that effort as one vehicle to advance the goals expressed in your letter, so we will be working on that immediately.

I also would like to take a second to talk about the 911 system. I think Jack has done a terrific job in explaining how basically it works. I would point out, just for point of emphasis, that one of the things that makes this problem difficult is there is no national unified emergency system. Even within the category of enhanced services, there are any number of variations on the basic model.

Sometimes a local telephone company is in full control of the location data base. Sometimes that data base is separately provided and resides within the control of the PSAP itself. Sometimes there is no such data base at all. Sometimes it is supplemented with computer-assisted dispatch technologies that do everything from keep track of the closest fire hydrant to keep track of whether that house has called before, whether there are toxic materials in the

area, et cetera. So there are any number of variations on that and we need to keep that in mind.

I would just divert for a second to supplement something Jack said that you may not be aware of. In the cellular phone context, there is a regulatory proceeding underway to bring enhanced 911 functionality like was described here to wireless. As of April 1 of, I think, 1998, cellular carriers were required to implement phase one of that enhanced 911 service, which means cellular calls should be able to transmit information about at least the cell from which the call came from and the caller's call-back number. That is being deployed, and in some instances even been tested, by the Telco Year 2000 Forum and ATIS and fixes that are necessary have been developed and are beginning to be deployed.

Phase two of 911 for wireless will come too late for this problem, but by 2001, we hope that technology will allow you to get the location within 125 meters of the actual phone itself. So I just wanted to make you aware of those efforts.

Last, I wanted to make you aware that there is a movement in the Congress to nationalize 911 as the national emergency number, as I think Jack sort of alluded to, that 911 right now is somewhat discretionary within States and localities and not everyone actually uses 911 as their emergency calling system. Indeed, I caution consumers with respect to wireless services, rarely is 911 actually the number that you will use to get an emergency service and you would be well advised to check with your carrier.

For example, AT&T's wireless mobile service, which I discovered recently, if you dial 911, you will get nothing, but if you dial 9 by itself and leave it alone, you will get emergency services, and I would not have known that, and did indeed when I was trying to use it, until I had spoken with them, so another caution.

I would also like to describe very briefly the 911 system and use slightly different components simplistically to give you an illustration of both where I think the problems and challenges are, and second, where I think we may have venues for attacking this problem.

I would break the emergency communications system down into three pieces, and I will borrow Jack's chart, with his indulgence, to make these points. There is the first phase, which I consider to be just 911 call delivery, getting the call from the phone to the PSAP. The second area is call processing at the public safety answering point. Third is the wireless dispatch component used to deploy emergency services to the location. And fourth is the emergency alert system, the use of broadcasting properties and cable systems to alert the public to national emergency, which are frequently used in times of weather emergency or other local crises.

With respect to call delivery, I think as you rightly stated in your opening statement, Mr. Chairman, that is largely within the control of the telecommunications companies. The public switched telephone network and up through the E911 tandem are things that the phone companies take direct and immediate responsibility for, and when we report on the general positive progress in the telecommunications industry with respect to that network, I think as Jack alluded to, as well, we would include those components.

So we have, again, as we used with the telephone system generally, guarded confidence about that dimension of the system. In fact, in the telecommunications industry tests that were conducted this spring by the industry, they included testing of functionalities of the 911 specific component.

With respect to the second dimension, this call processing area, that is, to be simple, a host of computers that do any number of variations on data bases, lining up information associated with the telephone number. We tend to put most of that information in the category of customer permit equipment. Again, as Jack mentioned, this is stuff that State and local governments buy and own and make choices about how sophisticated or unsophisticated it is. They are provided by separate vendors in most cases. Indeed, the two leading manufacturers, which I believe are Positron and Plant Equipment, Incorporated, produce that equipment. So that problem is the classic problem of CPE, trying to get individual institutions to address those problems and get with their vendors to remediate the situation.

We have some confidence that, with respect to that equipment, fixes have been developed and are available. I think that the challenge is going to be largely in deployment.

Also, I wanted to highlight another venue we have for potentially attacking this problem, which we have already made some efforts to utilize, and that is that the telephone companies. Because of historical legacy, telephone companies often have service and maintenance contracts with public safety answering points for not only the telephone side but some components of the call processing within the PSAP. In fact, what NRIC did was attempt to survey its members, that is, the eight largest telephone companies, and say, hey, look at your service contracts and tell back to us what efforts you have engaged in remediation because you are one of the parties that they are likely to hire to do this.

They come up with a number somewhere in the neighborhood of 7,000 PSAP's, 6,739, and I would point out the discrepancy in the numbers FEMA reports and we report is explainable by the fact that FEMA's numbers come from primary PSAP's and often localities will have secondary PSAP's and our numbers probably capture those secondary PSAP's, as well. These are institutions that the phone companies have contracts with.

That is where you get the reported number of 35 percent remediation, from the phone companies who are reporting on their efforts pursuant to their contracts for that equipment. And again, as you correctly pointed out, that probably only gets you sort of midstream into that processing component and there are probably other components of that processing component and then the dispatch side which are not captured by that number.

That takes me to the dispatch side. Once you get past the PSAP processing, it is time to deploy a fire truck, time to deploy an ambulance. There is wireless communications equipment utilized for that purpose. Two major pieces there, one in which the FCC has a great deal of control over, which is frequencies and the allocation of frequencies and management of those licenses and the people who have them as licensees. But, of course, the airwaves are the airwaves. As far as I know, they do not have a Y2K problem yet.

But the central problem is probably in the equipment that is being utilized, and we have done lots of assessment with some of the basic kinds of wireless equipment in our normal course of work with wireless manufacturers. The manufacturers report relatively positive news about wireless equipment. Most of it being used by public safety authorities do not contain the more sophisticated date-sensitive information and are likely going to be capable of transmitting basically a telephone call or a dispatch call. But, nonetheless, that has to be checked and we do not really have any tangible information with respect to it.

Finally, a part that Jack did not refer to which does come under our jurisdiction, as well, is the Emergency Alert System. You have seen it. It used to be referred to as the Emergency Broadcasting System and you got that annoying beep when they tested it. We do not use that anymore. There are now more sophisticated technologies to scroll information across television screens and audio alerts over the radio. Cable companies for the first time are required by law to provide these warnings, as well.

Because these systems are very new—we have required these only over the last couple of years—Y2K has been a prominent concern in the deployment of that equipment from the get-go and we are pretty confident that the Emergency Alert System is likely to function and function well, and we are also confident that it has a lot of redundancies. That is, in any given neighborhood, like our own, there are multiple television and radio stations and if one or two of them were to have a failure, you are likely not to be fatally excluded from news and information.

I will stop there and am happy to take any questions you might have.

Chairman BENNETT. Thank you very much.

[The prepared statement of Mr. Powell can be found in the appendix.]

Chairman BENNETT. Between the two of you, I think you have covered this very well. Let me just emphasize again, so that I understand, if there is a failure, the call will still go through?

Mr. BROCK. If there is a failure on the——

Chairman BENNETT. That is assuming that you get a dial tone.

Mr. BROCK. Yes. In most cases, we believe the call will go through. In some cases, if the whole phone is replaced by a computer, the call may not go through in the PSAP, but we do not believe there are that many systems that use that.

Chairman BENNETT. And if it goes through, it will be handled the way a cellular call is handled now?

Mr. POWELL. Probably, in all likelihood. Before the PSAP system was created, I think the late 1960's or early 1970's, essentially what you have is a trained operator whose purpose it was to keep you on the phone and collect that information and then be simultaneously dispatching that information.

I suspect if there were a collapse of the automated assistance of that system, you would essentially revert back to sort of pre-PSAP era in which the training and the abilities of your operator become much more critical and central.

The second backup which we should allude to is PSAP's were designed for efficiency. There are numbers to call the police depart-

ment directly. There are numbers to call your fire station directly. In the contingency phase, we need to make sure that one thing we consider is making sure the public knows that there are alternate ways to call for emergency services, should it have trouble with basic 911.

Chairman BENNETT. You have come back to one of my recurring themes as people say, well, what should the average America do, and I think the answer you are giving here is that the average American should first call his local official and do a little analysis by himself as to how far they are along on the readiness scale, and then, second, record these emergency numbers so that if the 911 system gets jammed, and that is what I see happening from your testimony.

You have all of these calls coming in and they end up with an operator and pretty soon you are on hold or you have busy signals, the kinds of things that were the plague of 911 in the early days that have been eliminated by the PSAP come back, only they come back with a vengeance now because the traffic is much higher than it was in the early days of 911.

So as a personal contingency plan in my own household, I need to get the number of the local police station directly so that if I get hung up on 911, I can still make that call and still get through.

Mr. POWELL. And I would just emphasize another point which we alluded to in our consumer tips in the telecom report that we issued a few months ago. With regard to 911 services, time is more critical than anything, and I would urge consumers who often wait until the very last second before they decide someone is hurt enough or ill enough to make a call, that understanding that it could take longer than it might normally take, I think at the first sign of trouble, one would be well advised to get on the telephone and accommodate for that potential lag in time.

Chairman BENNETT. That is a good piece of additional counsel and information. We thank you both and appreciate your testimony and your effort in this area.

Mr. POWELL. Thank you.

Mr. BROCK. Thank you.

Chairman BENNETT. We will go to our second panel now. On this panel, we welcome Mr. Stephen R. Colgate, who is the Assistant Attorney General from the Department of Justice. He coordinates the President's Working Group on Law Enforcement. We look forward, Mr. Colgate, to your testimony about the Justice Department and the working group's outreach efforts.

Mr. Colgate is joined by Mr. Harlin McEwen, who is the Deputy Assistant Director of the FBI. He will testify about those FBI information systems which support State and local law enforcement agencies. He is also a former chief of police, which I think will give us an opportunity to draw on that expertise.

Finally, we have two witnesses from the front line of law enforcement, Chief John S. Karangekis of the Wethersfield, Connecticut, Police Department. He serves as President of the Connecticut Police Chiefs Association. He will be joined by Chief Jim Brown of the Hudson, Ohio, Police Department, who is President of the Summit County, Ohio, Police Chiefs Association.

From the Department of Justice to the FBI to two chiefs of police who are on the front line every day, we appreciate your being here. Mr. Colgate, we will start with you.

STEPHEN R. COLGATE, ASSISTANT ATTORNEY GENERAL, JUSTICE MANAGEMENT DIVISION, DEPARTMENT OF JUSTICE

Mr. COLGATE. Thank you, Mr. Chairman. My name is Steve Colgate and I serve as the Assistant Attorney General for Administration and also the Department's Chief Information Officer. I am pleased to share with you some observations about Y2K readiness in the State and local law enforcement community.

I welcome the participation at this hearing of the FBI's Harlin McEwen. As you have pointed out, Harlin was a former local law enforcement officer and is a key player in the development and deployment of the Department's Criminal Justice Information System.

Your invitation identified five subject areas, and I see them from two separate viewpoints. First, I have the viewpoint of my own role in the management of the Department of Justice. Then I have the viewpoint of the working group that I lead under the President's Council for Y2K Conversion. That working group has a very broad scope that involves more than policy and highway patrol agencies and includes law enforcement in the context of such Federal regulatory activities as clean water.

First, from the viewpoint of the Department of Justice, the Department has a mutually dependent relationship with State and local law enforcement agencies. We share concerns for smooth operational business continuity at the year's end. However, because those relationships are so numerous and diverse and so many of the information interactions are so sophisticated, it is proper for DOJ's Y2K readiness responsibility to be in the Department's bureaus and divisions in all of our components. They are responsible for all aspects of their missions, including addressing mission partner readiness. I am pleased to tell you they have been working very hard for a great many months and are in a very good position to make an uneventful transition at this year's end.

We are also emphasizing continuity of operations planning, in which our components are layering and laying the groundwork to deal with any business process anomalies that might occur over the new year period and in the days and weeks to follow. As of April 28, 1998, 93 percent of the Department's mission critical systems are compliant, and I am very pleased with that.

Your invitation addressed specifically the Y2K readiness of State and local law enforcement. I see this as having two principal dimensions. One is the awareness relative to their mission partner interactions with the Department. The other is awareness relative to the activities that are purely and entirely State and local, not involving the mission interactions with the Federal Government.

DOJ strategy has been to concentrate on the operations in which we are a party. In so doing, we have encouraged our State and local mission partners to follow our lead and look to all of their operations, including those that do not involve the Federal Government. Over the past 10 months, the Department has undertaken a Y2K readiness awareness with its mission partners in all areas,

especially in law enforcement. That campaign has included the Attorney General herself, and the FBI has have been working hard at communicating Y2K awareness to all of its partners, which are all the 50 States and territories.

My feedback indicates that State and local officials know well the two things that are of paramount importance to the Department, namely, that the Department is doing its own Y2K readiness so that States can depend on our systems and the States must do certain things to ensure their end of the partnership, as well. Those include data exchanges as part of information system operations and are being tested as a part of the Department's overall Y2K readiness validation and verification process. In that context, I believe that it is important to bear in mind that our principal law enforcement interfaces are with State and local officials on whom we rely for reaching local officials in their many small jurisdictions.

From my second viewpoint as a leader of the Working Group for Police, Public Safety, Law Enforcement, and Criminal Justice of the President's Y2K Conversion Council, I have an interest in the unusually wide spectrum of entities that include not only those that are part of the State government but those that exist at the county, city, and township levels.

In the case of just police, the entities number in the tens of thousands because almost all the small villages and towns, like their big city brethren, have their own police departments. I believe that smaller police departments are very numerous and they tend to rely greatly on other local government entities for their information technology sources and support.

For all of our working group participants other than DOJ, I believe the Department of Transportation's Federal Highway Administration has the most potential impact on State and local, simply because of the issue of traffic control, and I think that they have done a good job in identifying the issues on traffic control.

I would like to conclude with some general observations. I have some concerns with many small rural departments that do not have their own expertise and rely on the infrastructure support from other units of government. Because of this concern, the President's Y2K Council, under the leadership of the Domestic Interagency Working Group, will sponsor a sector roundtable session with both the Law Enforcement Working Group and the Public Safety Emergency Management Working Group to discuss contingency planning and readiness.

In conclusion, I believe that the Department of Justice systems are in good shape and will meet the challenge of Y2K. There have been outreach efforts with our State and local partners and my informal discussions with some of the law enforcement associations indicate a good general overall awareness. However, more needs to be done, and to that extent, we will be working with the Federal Emergency Management Agency and the Public Safety Emergency Management Working Group to undertake a more thorough assessment of State and local readiness, and we will, of course, keep the committee fully apprised of our efforts.

Thank you for this opportunity.

Chairman BENNETT. Thank you very much.

[The prepared statement of Mr. Colgate can be found in the appendix.]

Chairman BENNETT. Mr. McEwen.

STATEMENT OF HARLIN R. McEWEN, DEPUTY ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. MCEWEN. Thank you, Mr. Chairman, and good morning. I am Harlin McEwen. I am Deputy Assistant Director of the Criminal Justice Information Services Division of the FBI. I apologize for my gravelly voice, but I am just getting over a case of laryngitis. This is the first day I have really attempted to try to speak publicly.

I am pleased to have this opportunity to inform you of the work that we have been doing at the FBI as it relates to assisting State and local law enforcement on the topic of year 2000 readiness and the criminal justice information systems. As you mentioned, I am a former city police chief of over 20 years and I currently serve as the Chairman of the Communications and Technology Committee of the International Association of Chiefs of Police, a position that I have held for 21 years.

I have been personally involved in educating and assisting State and local law enforcement agencies on year 2000 matters for the past four to 5 years. At the FBI, we have taken a very proactive role in keeping the Y2K issue before the States and encouraging them to plan for and institute changes to make their systems compliant with our nationwide system.

In the FBI advisory policy process, our primary interaction is with the State Control Terminal Agencies—we call them the CTAS, as you mentioned, another one of these little references—who are responsible for providing the appropriate interconnect with the FBI system and for providing the necessary Statewide systems and access for State and local agencies to the FBI system.

The following is a brief chronology of the actions by the FBI to assess the readiness of the State CTA's and to ensure that they were aware of the consequences if State systems are not ready for the date change. Starting in the spring of 1996, the FBI CJIS Division prepared a staff paper for the Advisory Policy Board Working Group meetings presenting the Y2K issue and proposing alternatives for compliance. The working group recommended converting all dates in the NCIC system, or National Crime Information System, to the Y2K format. This recommendation was approved by the APB at their June 1996 meeting.

In September 1997, the FBI CJIS Division and the Information Resources Division of the FBI hosted over 400 State and local criminal justice agency representatives at the NCIC 2000 Technical Conference in Tulsa, Oklahoma. At this conference, the timetable and formats for the Y2K date were presented and the need to plan for necessary changes was stressed.

On September 25 of 1997, the FBI CJIS Division sent a technical and operational update to all the States informing them of the timetable and the formats for the date changes.

In January 1998, the FBI surveyed the States and requested information regarding the readiness of the States for NCIC and Y2K

compliance. At the request of our Advisory Policy Board, the States were sent a letter explaining the Y2K schedule and the consequences of not being compliant with nationwide systems by July 1999. The reason for the July 1999 reference is that that is when we will be actually delivering our new NCIC 2000 and our new Integrated Automated Fingerprint Identification System and it is necessary for the States to be able to interact with those systems at that point in time in a Y2K format.

The letter enclosed a form requesting that the agency head sign a statement acknowledging that the schedule and the consequences are understood. All States responded with a signed statement. Unfortunately, the District of Columbia did not respond.

In December 1998, the District of Columbia Metropolitan Police Department contacted the FBI and indicated they were having difficulty with Y2K compliance and requested FBI assistance. The FBI CJIS Division and our Information Resources Division responded to the District with technical consultants and the conversion software developed by the FBI to convert NCIC dates.

Subsequent to this, the city government provided the Department with additional resources and we have been assured that the situation is now under control. This is particularly critical, because the District of Columbia Metropolitan Police Department provides the interface to our FBI system for all law enforcement agencies in the District. This includes all the DOJ components, such as the FBI, the Drug Enforcement Administration, U.S. Marshals Service, the Immigration and Naturalization Service, and the Bureau of Prisons. It also includes the Treasury law enforcement agencies such as the U.S. Secret Service, ATF, U.S. Customs, and agencies that are quite prominent in your traveling around, the U.S. Park Police and the Postal inspectors.

Between November 1998 and April 1999, the FBI has been conducting external interface checkout testing with all States. The States have been strongly encouraged to use this Y2K compliant data format in these tests. However, we did not make it mandatory, as some States are still in the process of converting their software or have contracts with work in progress to make their systems Y2K compliant.

In February of this year, the FBI hosted another conference of over 400 State and local criminal justice agency representatives at our Integrated Automated Fingerprint Identification System [IAFIS], technical conference held in Los Angeles. At this conference, again, the timetable and other issues related to Y2K issues were presented and the need to plan for necessary changes was stressed.

Between February and May of this year, we have started conducting site operational tests. We call it the SOT. Those States which did not use the Y2K compliant date formats in the EIC are now required to do so in these site operational tests.

In July, as I mentioned, we will be delivering the NCIC 2000 and IAFIS systems and we expect that they will be fully operational. Of course, at that time, the Y2K date formats are mandatory.

I will mention that the Attorney General has expressed continuing concern about the Y2K issue, and Mr. Colgate has mentioned it in his remarks. She had asked us at the FBI, because we do have

to be sure that this is going to be all working when this all happens, to take one extra effort, and yesterday, I spent a great deal of the day discussing with our FBI team how we were going to take one last effort to try to make sure that we have done everything possible to assist the State governments to be prepared.

So we have made the decision now that in the next 2 weeks, we will start sending out teams. We are planning on sending out five teams of two to three States a week and we expect that in five to 6 weeks, we will have visited every State once again, and we will, hopefully, complete that by late June and we will have a complete sense of whether the States are in final readiness.

I would mention that, again, our primary interface is with the States and their primary responsibility is to make sure that the State and locals will comply with their State formats, which will then, of course, come on to the FBI. We are prepared to offer assistance to all of these States and I think that what we have done and what we are doing are appropriate from the Federal Government perspective in our role in assisting them.

I thank you for the opportunity to give you this overview and would welcome any questions.

Chairman BENNETT. Thank you for your testimony and for your work. We will look forward to the results of that State-by-State survey that you just described to us.

[The prepared statement of Mr. McEwen can be found in the appendix.]

Chairman BENNETT. Chief Karangekis, we appreciate you being here and we will hear your testimony.

STATEMENT OF JOHN S. KARANGEKIS, CHIEF OF POLICE, WETHERSFIELD POLICE DEPARTMENT, WETHERSFIELD, CONNECTICUT

Mr. KARANGEKIS. Thank you, Senator. Basically, what I have heard this morning in previous testimony pretty much parrots many of the things that I have in my short presentation.

An informal survey of a cross-section of police agencies in the State of Connecticut reveals that agencies vary in their level of progress to remediate Y2K issues prior to the turn of the century. There is consensus that it is imperative that each law enforcement agency show due diligence in their efforts to mitigate any adverse impact resulting from non-compliant technology. It is believed that the Connecticut experience is probably similar to that of all other law enforcement agencies throughout the country, and I am beginning to pick that up as I hear some of the testimony.

The majority of large cities and towns in Connecticut appear to be much ahead of some of the smaller police departments and communities. It is clear, however, that law enforcement agencies recognize, at this point, particularly, the importance of due diligence and are actively addressing those issues in their own communities, again, I repeat, at various levels of completion.

A recently released Y2K readiness report distributed by the State of Connecticut, the Department of Information Technology, regarding Y2K remediation efforts gives strong indicators that they anticipate there will only be a minimal adverse impact during the turnover. That is based on their projections that most of the State

will have addressed all the technological issues, the interfacing, both at the State, Federal, and local level, obviously, and that these systems will, for the most part, do what they are supposed to do.

Most significantly, it appears that in our State, who we have just recently redone the entire 911 system with both new hardware and new software—that is being done as we speak and those systems will be turned on sometime during the late summer, I believe. They are all in place, local PSAP's. They have not been interconnected yet because there is still some work going on on the technology and servicing end, but this system in Connecticut is Y2K compliant. The issue, of course, is again to make sure that any system or technology that those systems interface with is also Y2K and we are in the process of doing those things now.

Like many communities, the town of Wethersfield has initiated a town-wide year 2000 readiness. We have committees that have been set up. Each department in our town government as well as State government determines their own issues. They determine what their technology is all about. They go about getting assistance to determine whether, in fact, their hardware and software are all Y2K compliant.

It appears at this time that approximately 80 percent of all the towns in the State of Connecticut, town and police technology, including computers, telecommunications, alarm systems, internal data systems, and records systems are Y2K compliant. Progress is being made through follow-up, software upgrades, and/or replacement.

Progress is being made. However, the one thing that we have noticed is that it has become increasingly difficult for us to get specific answers from some of the vendors, some of the manufacturers, particularly in the telecommunications area. There is a reluctance on their part to specifically say, "You are all set." It is very, very difficult to get them to put it on paper. They do couch their words when they talk to you, and even when they come out and do an assessment, the report you get is permeated with disclaimers. That seems to be a problem and we are hoping that that is going to rectify itself as time goes on.

The one thing that I have noticed and have particularly taken concern with is that we perhaps started a little too late to deal with Y2K. We probably should have started 5 years ago, because now the situation is that everybody is rushing to make sure that they are going to be adequately in place at the time that the century turns over.

Contingency planning, obviously, is the most important thing for us at this point because of the unknown factors here. In the police service, contingency planning is something that we do frequently, Statewide, locally. We have had disasters before. We have had power outages before. We have had situations where we have had to come together. I feel reasonably certain that at least from the point of responding to public safety situations in local communities and at the State level, that we will be able, in fact, through our contingency planning and replacement of certain kinds of equipment that is not affected by Y2K bugs, we are going to be able to deliver police services, perhaps at a slower rate and dependent on how many failures may occur, if they do occur.

I believe that we have to be very diligent in our efforts. Time is short. There are some law enforcement concerns that are very paramount, particularly for smaller police departments. I would name some of those as the reluctance of vendors to guarantee Y2K compliance clearly. We concern ourselves about the reaction of the community when the time comes for the turnover. We almost anticipate that at 1 minute after midnight January 1, 2000, that everybody is going to be picking up their telephone and trying to call all public safety points to see if we are in business. That in itself would cause some problems.

There are significant costs associated with contingency planning and staffing and costs for updating hardware and software. That is a difficult situation, particularly for small communities where there has not been much significant long-term planning for these things, and that is why I say I am sorry we did not start these things several years ago.

But we are prepared. I believe that any situations that occur will be minimal, but we have to continue to pursue Y2K compliance in all areas of public safety and I believe that we will be able to do that if everybody wakes up. Thank you.

Chairman BENNETT. Thank you very much. I have always said that the way to solve your Y2K problem is very simple. Just make sure you start in 1994 and you will not have any difficulty.

[The prepared statement of Mr. Karangekis can be found in the appendix.]

Chairman BENNETT. Chief Brown.

STATEMENT OF JAMES N. BROWN, CHIEF OF POLICE, HUDSON POLICE DEPARTMENT, HUDSON, OHIO

Mr. BROWN. Good morning, and thank you, Senator Bennett. I am honored and privileged to come before you this morning to provide you with a municipal law enforcement administrator's perspective concerning Y2K and the contributing factors that have led to varying degrees of apathy from within the law enforcement profession, which has not emphasized a strategic response in the form of a community-wide contingency planning objective.

As the Chief of Police for the city of Hudson, Ohio, a community of approximately 23,000 residents located between the cities of Cleveland and Akron, I have oftentimes found myself having to contend with problems categorized in broad terms as safety and security matters. Safety and security can be compromised if we trivialize or ignore various indicators of an impending problem or crisis, and Y2K presents classic indicators of such a nature.

Basic utility services alone are critical components of a community's safety and security, and although their dependability is remarkable, it has correspondingly lulled many of us into a false level of expectation, whereby failure is thought of as being virtually impossible.

In the absence of active discussion at various association meetings, regional conferences, et cetera, and the virtual non-existence of Y2K-related training sessions specifically designed for law enforcement to address Y2K from something other than a technology perspective, it is unlikely that most agencies have even discussed the possible implications that Y2K poses. Most law enforcement ad-

ministrators, on the other hand, are sufficiently motivated to prepare their respective agencies and communities if they are exposed to some basic guidance and direction that originates from within our own profession.

The law enforcement profession is equipped with vast media resources through its many associations, and yet, with few exceptions, there has not been much substance in coming to terms with contingency planning.

There is a considerable level of apathy from within the profession, as I mentioned, concerning Y2K and a variety of factors have influenced this response. There is considerable contradiction and rhetoric amidst the voluminous amount of documentation being made publicly available, which I believe have clouded the issue and drastically minimized Y2K's credibility as a potentially serious problem.

Terminologies such as "minimal impact" or "sporadic disruption" have created a comfort factor for skeptics in all professions. Sporadic almost implies the existence of some distant community on the other side of the globe to which we have no allegiance or direct responsibility. The immensity of our communities oftentimes jades our sense of the enormity of the United States. The perspective changes rather dramatically, however, when I suggest the placement of a straight pin into one's hometown on a wall-sized map of the United States and I pose the question, "Could your hometown be Sporadicville?" Perhaps it is the absence of the threat of structural damage and property destruction that has caused many law enforcement administrators to downplay the significance of Y2K. Perhaps it is the absence of a sustained media campaign to bring Y2K implications to the attention of the American public, which to date has been limited. One local television reporter representing a large network was advised by management that the Y2K issue was too frightening and might induce fear and cause panic, this from the same network that daily provides graphic pictorial details of human misery and death worldwide.

Several weeks ago, I forwarded a letter to the general managers of 12 different major media outlets advocating the necessity for additional media exposure. To date, I have received not so much as a single response.

There is a relatively small percentage of communities and law enforcement agencies throughout our country who have experienced crisis in its infinite forms, managed it effectively, and are thoroughly prepared to implement a successful contingency plan at a moment's notice, and then there are all the rest.

Even a perfect plan loses its luster and brilliance if the true beneficiaries of its development and execution, our residents, are unaware as to how they summon critically needed emergency services in the absence of a functioning telecommunications network; the availability of predetermined shelters, if they have exhausted their own resources or their homes are and/or become uninhabitable; and we have failed to provide simplistic, yet essential, guidelines as to how the average family can sustain itself in the absence of government assistance.

The character, the grit, and the determination of the law enforcement profession, continually faced with challenge and adversity,

lend themselves to a successful outcome regardless of the nature of the event. The local law enforcement agency is in some respects the first and last line of defense for our communities and they will be looking at us, as law enforcement administrators, for direction and guidance as 1/1/2000 approaches. The law enforcementprofession must recognize this responsibility and meet the challenges that it presents.

Be there no mistake, however. Our dependability and reliability is, as always, rock solid, and with special regard to Y2K, it is the lone absolute amidst a world of uncertainty. Thank you very much.

[The prepared statement of Mr. Brown can be found in the appendix.]

Chairman BENNETT. Thank you all very much. We have just started a vote, so I have my eye on the clock perhaps a little more than usual.

Let me go back to a comment you made, Mr. Colgate, and get everyone's quick response to it. You mentioned traffic control. Does anyone have a sense of how reliable the traffic systems are, the signals are and so on are? Has anybody looked at that? Yes, Chief Karangekis?

Mr. KARANGEKIS. Senator, I can only speak for the State of Connecticut, only because within the past few days, we have networked with State traffic control and they are of the opinion that they are going to be ready, that they feel they are going to be able to handle the traffic function. I am hoping that that is a correct statement.

Chairman BENNETT. I was struck by your comment about everybody picking up the phone after they have celebrated and calling to make sure everything works. This can become a self-fulfilling scenario for panic. Gee, everything does not work and the whole thing must have failed, and it did not fail, it is just overloaded.

So we come back to the whole question that you were addressing, I think, Chief Brown, of getting the media to understand what is real, what is not. This is an unfair generalization, but elements of the people in the media seem to swing between this is the end of the world as we know it, or you are wasting our time to even hold these hearings because everything is going to be fine. The reality, of course, is between those two extremes. We could get some help from people in the media if they could just be a little more measured in their reporting, but somehow, being measured does not fill airtime. You were going to comment on that further?

Mr. BROWN. As I stated, I think the local police administrators are anxious to learn as much as they possibly can about the whole issue. Furthermore, I think the communities are looking for the leadership and guidance from, in some jurisdictions, it is the law enforcement agency head for guidance. And I think it is important that, obviously, we spend the time in meeting with our respective communities to bring them into an awareness level, teach them how to prepare, and some guidance, as was just mentioned, in terms of suggesting to folks that they not pick up the phone routinely to make sure that the system is working, et cetera. So I think the public is looking for our assistance in that regard.

Chairman BENNETT. Mr. McEwen, can you give me the typical failure mode for crime information systems? In the worst case, what could happen, arrest warrants or a person's information be

erroneously dropped from the system? Is that something that could happen?

Mr. MCEWEN. Well, I do not think so, because the main data base, we maintain, and we have complete assurance that our systems are Y2K. It is the connectivity that is the more dangerous that we are trying to address. The scenario is that you started back with the earlier panels the discussion about 911. It all starts kind of in the beginning at the local level and all of those connections until it gets to the FBI, like the NCIC system, where they are checking for a wanted record on an individual, every one of those links has to work.

The worst case scenario is that any one point in that whole communications link fails and they are not able to get timely information. We have pretty good assurance, as I said, that the States are prepared to handle that. What we really do not have a good sense of, and one of the things that we will do in our visits in the near future will be to ask once more, how well are the States set in their readiness with the local agencies, such as these chiefs in Connecticut and in Ohio.

Mr. COLGATE. Mr. Chairman, if I could just add to that——

Chairman BENNETT. Sure.

Mr. COLGATE. In my discussions with John Koskinen on the Council, the best way I can describe this is that we are very confident in the Federal system, that the Federal system will be up and running. But my concern is, to give you an anecdotal example, is that you have a very small police department, let us say less than half a dozen sworn officers, and they do a traffic stop and they have a particular individual, and because they are not Y2K ready, they will not impact the Federal system. The Federal system will be able to operate.

What I am concerned about is the officer on the street not having the ability to do a search about somebody who he has temporarily detained and ascertain who is this individual? Does this individual have a criminal history? Am I exposing myself and the community to danger? The system will be there and available to him. It is just our concern that he will not have the capability to make that query.

That is why the Attorney General has asked the FBI to really focus its efforts now and really get out there and deal with the States who we hope, in turn, will be that leveraging agent down to that very small local police department.

Chairman BENNETT. Thank you for that. I would hope that as you go through this assessment on the part of the FBI under the direction of the Attorney General, that you try to put together a road map of where the remaining problems are and fairly firm indication of who needs help.

We are getting a general picture here, which, frankly, is not unlike that which we get from the business community as a whole. That is, the big companies are probably going to be all right. You are telling us the Justice Department is going to be all right. You are telling us the State of Connecticut is going to be all right. It is the smaller to medium-sized companies, and from the testimony overall that I am hearing here, it is the smaller and medium-sized law enforcement agencies that have the most problem.

But we do not know. We are guessing. We have two chiefs here who tell us that they are going to be fine, primarily because they are doing the prudent thing and getting contingency plans in place so that if the connectivity that you talked about does not work, they can still see to it that their law enforcement is available.

It is the fact that we are flying blind in these areas that causes us the concern, and I would hope that the Justice Department would look to try to construct that kind of road map and say, all right, here are some more specific statements of exactly where we are and what we are doing.

Mr. COLGATE. If I could just respond briefly, Mr. Chairman——

Chairman BENNETT. Certainly.

Mr. COLGATE. I agree with that assessment. We have met informally with the Federal Emergency Management Agency, and because of the smaller communities, we are dealing with very small law enforcement operations, usually, you have sort of a combined emergency response capability in those very small rural areas. We are going to be entering into a partnership with FEMA to engage in a telephonic survey to really focus on some of those smaller locations so that we can get a better sense and get a better assessment of the issues that they face.

We have a good window with the FBI because of the fact that we constantly have a window into their operations at the State level. But we hear you loud and clear and we will be working with FEMA to really focus on those smaller communities where there is a combined emergency/public safety response to get a better snapshot.

Chairman BENNETT. Finally, and then we will have to adjourn the hearing, Mr. McEwen, you have talked about people who have a very late timeframe to get this under control, and I would hope as you do your State-by-State assessment you would focus on that, because the fear we have in this committee is that a lot of people who give us their assurance, yes, we will be ready, are saying, we will be ready because things will be delivered to us in October or November or by the 15th of December and so on. Life being what it is in the IT world, something that is delivered in November is not going to be reliable in January.

The President set March 31 as the deadline for the Federal Government to be compliant. There are some Federal agencies who missed that. Then we are saying, well, as a backup date, June 30, or the second quarter. That is really as late as we can go with the big systems.

Now, there may be some small systems that could survive if the fix shows up in August or September, but as you go around, try to make a list of those who are saying, everything is going to be fine and it is going to show up on Halloween. That is really pretty scary and we would like that information, if you would share it with us.

Mr. MCEWEN. I totally agree with you, Mr. Chairman, and I think that is exactly why the Attorney General has asked us to, one more time, just go out there. We are convinced that there may be some cases where they have told us that everything is fine and when we get there, they are going to say, well, we are still working on it and we are not quite sure. We need to know that, so we hope we can help them with that.

Chairman BENNETT. We thank you all. The committee is adjourned.

[Whereupon, at 10:52 a.m., the committee was adjourned.]

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

Our hearing today marks the second time in six months that this Committee will address the important topic of Y2K emergency preparedness. Our October 2, 1998 hearing focused on emergency management, and included testimony from FEMA, the National Guard Association, the National Emergency Managers Association, and the National Governors Association. Today we will concentrate on the impact of Y2K on two specific areas of emergency preparedness: 911 systems and local law enforcement. We touched somewhat on these areas during the October 2 hearing, but today we address these issues with a heightened sense of concern.

Our concern about these areas is heightened for two reasons. In a report released last month, the Network Reliability Interoperability Council, or "NRIC", estimated that only ten percent of the Public Safety Answering Points or "PSAPs" where 911 calls are processed were prepared for Y2K. In an updated report received from the FCC yesterday, the Committee was informed that this number might now be as high as 35 percent. However, it should be noted that this refers only to the equipment provided to the PSAPs by the telephone companies.

There is still a large amount of equipment and information systems utilized within PSAPs about which little are known. An ongoing survey being conducted by the U.S. Fire Administration about overall readiness of 4,300 PSAPs indicates that overall readiness is only about 17 percent. Survey results indicate some strong concerns about funding on the part of the PSAPs.

Keep in mind that in the United States, there are approximately 300,000 calls for emergency assistance made via the 911 system each day, not counting the additional 86,000 911 calls made daily from cellular phones. That is over 110 million 911 calls made per year. If problems within the systems supporting these public safety answering points are not properly addressed, these systems will fail, leading to degradation in the processing of 911 calls.

I would like to announce that Senator Dodd and I are jointly sending a letter to Commissioner Michael Powell of the FCC, who is here with us today, and Administrator Carrye Brown of the U.S. Fire Administration asking that they work together to identify those PSAPs that are not yet prepared, and those who have not yet responded to the Fire Administration's survey. We have also asked that they provide this information to the appropriate 911 commissions, state Y2K coordinators, or other appropriate regulatory body governing those PSAPs. Hopefully this will help the states and local jurisdictions identify potential problems so that help can be provided to those that might need it. There may very well be some people out there that have a problem, but don't yet realize it, even at this late date. The supervisor of one PSAP told Committee staff that the radio system in his dispatch center required a $60,000 patch. Without the patch, they would have been unable to communicate with emergency service units at all.

In regard to local law enforcement, the Committee has noted the absence of any overall assessment of the Y2K status of our nation's local law enforcement agencies. At the federal level, we have captured much information about our federal law enforcement agencies within the Justice Department and Treasury Department, such as the FBI, DEA, Customs Bureau, ATF, and Secret Service. This information has come to us through the quarterly OMB reports, and the work of the Inspector General offices of various departments. The news about these agencies is very good. If not already completely prepared, they are well on their way to being so, and we have every confidence they will be ready to meet their challenges on January 1, 2000. However, we are concerned about the lack of information on the segment of law enforcement that our citizens rely on most in their everyday lives, and that is

the local law enforcement sector. This includes approximately 17,000 police and sheriff's departments across the country.

As I have emphasized previously, we don't want to overstate the problem, or needlessly incite public panic. We have no reason to believe that our emergency service departments are not taking very seriously their responsibility to prepare for Y2K. We recognize however, that they are highly vulnerable to Y2K both in the 911 area and other areas of vital information technology. We are especially concerned about the lack of assessments of local law enforcement preparedness. Due to the lack of any hard data, we are unable to accurately make any statements about the level of preparedness in this area. As such, we find it necessary to hold this hearing today.

Law enforcement agencies at the federal, state, and local level rely on a wide variety of criminal information data bases in order to safety and effectively do their jobs everyday. The National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), the El Paso Intelligence Network, (EPIC), and the Narcotics and Dangerous Drugs Information System (NADDIS) form the backbone of crime information systems at the federal level. Some of these systems, particularly the National Crime Information Center and National Law Enforcement Telecommunications System also function as vital tools for all state and local law enforcement. Additionally, there are similar systems managed individually by each of the fifty states, as well as numerous regional crime information centers upon which local law enforcement agencies rely. Each police department also maintains its own arrest and criminal record systems. These systems play a vital role in increasing officer safety and the safety of the public, and enable the police to rapidly identify suspects and solve crimes.

We hope that this hearing will help "turn up the heat" as one might say in police jargon, and to encourage more active assessments in these areas.

The events in Littleton, Colorado last week stand as a sad and tragic reminder of the importance of our topic today. Before we begin, let me ask that we all keep the victims, their families and friends, and all those effected by that incident in our thoughts and prayers.

PREPARED STATEMENT OF JACK L. BROCK, JR.

Mr. Chairman and Members of the Special Committee:

Thank you for inviting me to discuss the impact of the Year 2000 computing challenge on the nation's emergency and state and local law enforcement systems and our review of the Department of Justice and the President's Council on Year 2000 Conversion efforts to facilitate remediation and contingency planning and to gauge the Year 2000 readiness of these two important sectors.

Briefly, we found that

- Limited information is available about the Year 2000 status of 9–1–1 call answering sites throughout the nation, known as Public Safety Answering Points (PSAPs). The Federal Emergency Management Agency (FEMA) in conjunction with the National Emergency Number Association [1] has surveyed 4,300 primary PSAPs on their Year 2000 readiness; however, as of April 1999, only 18 percent responded. Of those that did respond, only 16 percent reported that their systems were compliant. However, the majority of the rest of the respondents reported that they will be compliant by 2000.
- Little is known about the status of state and local law enforcement agencies. No assessment surveys have been conducted. Last week, the Chairman of the working group focusing on law enforcement for the President's Council on Year 2000 Conversion informed us that such an assessment would soon be initiated in cooperation with a follow-on FEMA assessment of emergency services.
- Outreach efforts by FEMA, the Federal Communications Commission (FCC), the National Emergency Number Association, and other organizations have been fairly extensive, ranging from the development of contingency planning guidance to the hosting of forums for the 9–1–1 community on meeting the Year 2000 challenge.
- Outreach efforts by Justice generally have been targeted to raising awareness and, with the exception of the Bureau of Prisons, largely ad hoc in nature.

To prepare for this testimony, we reviewed the FCC's March 1999 report on Year 2000 readiness in the communications sector; transcripts of the FCC's emergency services forum held in November 1998; and the April 1999 Network Reliability and Interoperability Council (NRIC) report on Public Safety Answering Positions. We re-

---

[1] This is a trade association seeking to foster the technological advancement, availability, and implementation of a common emergency telephone number system.

viewed test documentation prepared by Bellcore and the Telco Year 2000 Forum to assess the scope of Year 2000 interoperability testing conducted on both the local public network in general, and on the continued ability of this network to successfully process 9–1–1 calls for emergency services. Further, we reviewed information published on the Internet by manufacturers of computer systems supporting 9–1–1 sites as well as by the FCC, NRIC, FEMA, the President's Council on Year 2000 Conversion, National Emergency Number Association, International Association of Emergency Managers, National Emergency Management Association, National Association of Counties, National Public Safety Telecommunications Council, State of Minnesota, and the State of Texas. We also toured 9–1–1 sites located in Arlington County and Fairfax County, Virginia, and we interviewed members of the Telco Year 2000 Forum and staff at both FEMA's U.S. Fire Administration and the National Emergency Number Association.

We also reviewed available outreach strategies and plans for the Department of Justice and its component bureaus and documentation on actual outreach activities that they have conducted. We discussed with department and bureau officials their respective approaches to managing outreach activities, including outreach goals. Additionally, we attended meetings of the Police/Law Enforcement/Criminal Justice working group, reviewed documents prepared by the working group, and conducted interviews with the Chairman of the group. We performed our work in March and April 1999 in accordance with generally accepted government auditing standards.

FEDERAL EFFORTS TO ASSESS CONTINUITY OF 9–1–1 AND STATE/LOCAL LAW ENFORCEMENT SERVICES

For the most part, responsibility for ensuring continuity of service for 9–1–1 calls and law enforcement resides with thousands of state and local jurisdictions. Nevertheless, the success of these efforts is of great interest at the national level as these services are critical to the safety and well being of individuals across the country. Thus, the lack of status information has increased concern about which, if any, critical emergency communications and law enforcement systems may not be compliant in time.

The President's Council on Year 2000 Conversion was established in part to help provide leadership and work with state and local governments to address the Year 2000 computing challenge. Last April, we recommended that the Chairman of the Council develop a comprehensive picture of the nation's Year 2000 readiness, which would include identifying and assessing the Year 2000 risks within the nation's key economic sectors, including those posed by the failure of critical infrastructure components.[2] By gathering basic information on Year 2000 status and impact on public well being, the Council would be better prepared to advise any necessary action to mitigate risks.

In October 1998, the Council tasked each of its working groups to complete sector assessments. These assessments were to be based on an assessment guide developed with input from GAO and were to be conducted in conjunction with related umbrella groups and trade associations. The Council's Emergency Services working group, which is chaired by FEMA, was responsible for conducting the assessment of emergency services, including 9–1–1 services. Because of the reliance of 9–1–1 services on the public switched network, this particular assessment was also dependent on results of the assessment conducted by the Telecommunications working group, chaired by FCC. The Council's Police/Public Safety/Law Enforcement/Criminal Justice working group, chaired by the Department of Justice, was responsible for conducting the assessment of state and local law enforcement agencies.

The first report summarizing the results of the Council's assessments was issued on January 7, 1999. The Council's second assessment report was issued on April 21, 1999. After the first report was issued, we testified[3] that, while the study was a good step toward obtaining a picture of the nation's Year 2000 readiness, the picture remained substantially incomplete because assessments were not available in many key areas, including 9–1–1 and fire services. Also, some surveys did not have a high response rate, calling into question whether they accurately portrayed the readiness of the sector. We stated that the Council needed to remain vigilant and closely monitor and update the information in the sectors where information is available and obtain data for those where it was not.

9–1–1 SERVICES YEAR 2000 READINESS

9–1–1 is the standard telephone number most Americans dial to quickly obtain assistance from police, fire, or emergency medical service providers. When dialing

---

[2] *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships* (GAO/AIMD–98–85, April 30, 1998).

[3] *Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T–AIMD–99–50, January 20, 1999).

9–1–1, callers depend on the country's telecommunications infrastructure, a high degree of automation, and emergency dispatchers to ensure that emergency personnel can be reached when needed.

If Year 2000 issues are not adequately addressed, the response to an emergency could be degraded. Fortunately, a number of positive outreach efforts have been undertaken to assist local governments as well as telecommunications providers in preparing for the Year 2000. Unfortunately, with less than 9 months remaining before the millennium, the status of thousands of 9–1–1 answering sites is still largely unknown.

9–1–1 and the Year 2000 Problem

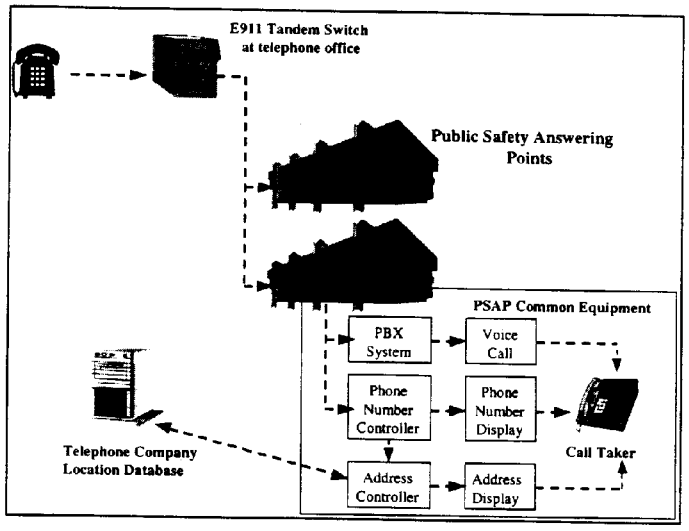
According to the FCC, about 90 percent of the population has access to 9–1–1 service and uses it to place most of the nearly 110 million emergency calls made in the United States each year. The remainder of the population, without access to 9–1–1 service, dials an ordinary seven-digit telephone number to contact emergency service providers.

The National Emergency Number Association estimates that there are approximately 4,400 primary PSAPs operating nationwide. These PSAPs, in turn, may have one or more associated secondary PSAPs. For example, the City of Falls Church, Virginia, operates a PSAP that is secondary to Arlington County's primary PSAP, 9–1–1 calls originating in Falls Church would be delivered to the primary PSAP in Arlington County. Following initial processing, that call would be forwarded for dispatch to the secondary PSAP operated by Falls Church.

The 9–1–1 system is a multi-step process that can vary from one PSAP to the next. However, 9–1–1 calls are initiated over the public switched network and most calls are made using "enhanced" 9–1–1 service—that is, service that uses automation to provide dispatchers with the address and telephone number associated with the caller.

The following figure depicts a typical 9–1–1 call.

Figure 1: Enhanced 9-1-1 Calling Process



Source: Network Reliability and Interoperability Council.

As the figure illustrates, the telecommunications component of the 9–1–1 system includes the public switched network, the local telephone office, and one or more PSAPs. A computer system at the local telephone office—called the E911 tandem switch—automatically routes incoming calls to the proper PSAP. At the PSAP, the call is recorded and information, such as the caller's location and directions on how to get there, is retrieved from a database normally provided by a local telephone company called the automatic location identification (ALI) database. Other equipment common to PSAPs are telephones, answering equipment, and personal computers.

The systems used by PSAPs and supporting telecommunications networks have processes such as day/time logging, call recording, computer aided dispatch, and records management systems that could be disabled by a Year 2000 failure. Should this occur, the following could happen.

- If the automatic number identification (ANI) database computers fail, 9–1–1 calls would not be selectively routed to a PSAP for processing, unless a default was established to route any call without ANI data to a specific PSAP. Depending on the service area, the loss of a 9–1–1 tandem switch could affect more than one million access lines.
- Also, if the automatic location identification database computers fail, the 9–1–1 attendant would get a voice path but not receive location data from the ALI database. The operator would then have to get location data from the 9–1–1 caller (which is routinely done with calls originating on wireless telephones) who may be confused or anxious.
- If the automatic call distributor fails, incoming calls would not automatically be delivered to available call takers.
- If a computer telephony integrated system (where the telephone has been totally replaced by computer) fails, the 9–1–1 attendant would lose all functionality and no calls would be received.

Another Year 2000-related problem is potential congestion in the public switched network arising from individuals making 9–1–1 calls to simply test the system. According to the Network Reliability and Interoperability Council, an increase in 9–1–1 traffic could result in callers getting circuit busy signals, put on hold for long periods, or disconnected.

Limited Information Is Available Concerning The Status of Year 2000 Readiness for 9–1–1

Successfully completing a 9–1–1 call next January 1—and taking full advantage of all the features of enhanced 9–1–1 service—is dependent on two major factors. First, the ability of the public switched telecommunications network to transmit the call and, second, the ability of the PSAP to process the call.

With respect to the public switched network, the Telco Year 2000 Forum on Intra-Network Interoperability Testing, which is made up of local exchange carriers representing 90 percent of all access lines in the nation, recently conducted tests to determine whether the public switched network could carry calls in a Year 2000 environment. The tests were performed on 54 different configurations of central office equipment that included a majority of the network components used in North America.

Only six Year 2000 problems were identified by the Telco Year 2000 Forum in over 1,900 test cases on these configurations, which involved 80 products from 20 different vendors. Assuming these tests were carried out effectively, their results provide some confidence that, if remediated, the public switched network should continue to function into the new millennium with no major service interruptions caused by Year 2000 dates. However, these tests did not focus specifically on 9–1–1 services and, as such, they did not test numerous "back end" systems that a PSAP might use, such as computer-aided dispatch systems, call logging systems, call recorders, and radios. PSAP operators are responsible for ensuring that these systems operate and interoperate properly after the date change.

The status of the ability of PSAP efforts to ensure that they can effectively process 9–1–1 calls is less clear. The Network Reliability and Interoperability Council[4] reports that major local telephone companies have taken action to ensure that PSAP systems they provide to their customers have been remediated. However, as of April 16, 1999, only 18 percent of 4,300 PSAPs had responded to a readiness survey conducted by FEMA and the National Emergency Number Association. Of the 766 sites that did respond, only 16 percent reported that they were ready for the Year 2000. Another 70 percent of those responding reported that they will be Year 2000 compli-

[4] The Network Reliability and Interoperability Council (NRIC) is a federal advisory committee that provides guidance to the Federal Communications Commission on how to promote the reliability of the public switched network.

ant in time for the millennium. Because of the low response rate, FEMA is planning to conduct telephone interviews with those sites that did not respond to the initial survey.

The Network Reliability and Interoperability Council developed its own assessment of PSAP Year 2000 readiness. The NRIC estimated that at present, fewer than 10 percent of the nation's PSAPs have completed upgrades of the 9–1–1 call processing equipment. However, according to the Council, many upgrades have been scheduled and should be completed within the second and third quarters of this year. The Council's evaluation did not address the Year 2000 readiness of any of the other equipment employed within the PSAPs that support call processing or personnel dispatch. The proper functioning of that equipment is the responsibility of PSAP managers.

Positive Outreach Efforts to Ensure
9–1–1 Year 2000 Readiness Are Underway

To help ensure that emergency services will be accessible after the century date change, many organizations are engaged in outreach activities to state and local governments and even the telecommunications providers that support networks critical to 9–1–1 calls. For example:

- In December 1998, FEMA included an informational Year 2000 brochure with a survey that was sent to primary answering points. It also developed Year 2000 contingency and consequence management planning guidance that specifically identifies 9–1–1 systems as being at risk because of the Year 2000 problem. This guidance was made available to state and local government emergency managers through a series of Year 2000 workshops held throughout the country. The guidance was also presented in a multi-state teleconference of state Year 2000 coordinators.
- The National Emergency Number Association is working to modify its technical standards, which cover a number of issues related to 9–1–1, to include Year 2000 compliance statements. The association is also advising its approximately 6,000 members to check their mission critical computers and equipment for Year 2000 readiness.
- The National Association of Counties has been working with the National League of Cities, the International City/County Management Association, and Public Technology, Inc. to address the Year 2000 challenge and its potential to impact services provided by local governments. Together, these organizations have developed and distributed over 20,000 copies of a Year 2000 information kit and have sponsored a nationwide Year 2000 satellite broadcast for local government officials and employees.
- On November 16, the FCC hosted a forum—attended by federal, state, and county government officials, telecommunications providers, and equipment manufacturers—on maintaining emergency response communications and potential Year 2000 issues. Topics discussed included potential Year 2000 threats to the system, strategies for averting those threats, and the need to convey the importance of the Year 2000 challenge to other emergency response organizations.
- The Association of Public-Safety Communications Officials International Inc., is planning to hold a Year 2000 symposium on May 20 and May 21 directed towards agency and company preparedness planning. Speakers will include officials from the FCC, the President's Council on Year 2000 Conversion and other federal government agencies, major utility companies, public safety communications center directors, volunteer associations and communications manufacturers and consultants.

STATE AND LOCAL LAW ENFORCEMENT
YEAR 2000 READINESS

Over 19,000 state and local law enforcement entities provide services to protect the American public. These entities vary greatly in terms of specific services provided, geographic coverage, and use of computer and communication tools. Management information systems, computer aided dispatch systems, and radio communications are typically used throughout the law enforcement community. All need to be thoroughly checked to determine their Year 2000 vulnerability and then fixed, if necessary.

Little Is Known About Year 2000 Status
For State and Local Law Enforcement Entities

The working group for Police/Public Safety/Law Enforcement/Criminal Justice has not done an assessment of state and local law enforcement agencies. Rather, its focus has been on increasing awareness through speeches, participation in conferences, and other similar activities. In the President's Conversion Council first report this past January, the working group reported:

> "Based on informal assessment information, there is a high level of awareness of the problem among non-Federal police/law enforcement entities. State police/law enforcement entities and departments in larger metropolitan areas are

making good progress. However, most departments at the county and municipality level lack the sophistication to assess the Y2K readiness of their service providers. These departments do not have their own, dedicated IT resources—money and professional staffing—and are instead dependent on the IT departments of the county, city, or municipality of which they are a part. Dedicated radio communications and dispatch systems are a concern for all police/law enforcement organizations and the working group is encouraging departments to focus on contingency planning in this area."[5]

The working group made no report in the second national assessment summary issued earlier this month.

Late last week, following our inquiries, the working group decided to develop an assessment of state/local law enforcement entities in conjunction with FEMA's efforts to develop more information on emergency services. The working group plans to conduct the survey by telephone to increase the response rate and to complete the survey by the time of the next sector summary report, which is expected in July.

Justice Outreach Efforts are Limited

According to the Justice CIO, the three department components with primary responsibility for outreach to state and local agencies are the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and Bureau of Prisons (BOP). With the exception of the BOP, neither the department nor its component bureaus have formal outreach programs with stated goals and defined strategies for actively reaching out to counterparts in state and local and international governments. In lieu of formal programs, the department and its bureaus are conducting largely ad hoc activities aimed towards increasing Year 2000 awareness.

Bureau of Prisons

In January, we recommended that the Bureau of Prisons proactively identify organizations needing assistance and share their experiences and lessons learned in remediating and preparing for Year 2000 problems.[6] The Bureau agreed and has established a proactive outreach program. For example:

- BOP established a formal outreach program with stated goals and defined strategies for reaching out to its counterparts in the state and local correctional community. BOP's plan called for this work to be conducted through professional associations, with an aim to deliver relevant information to corrections officials and to provide direct assistance where needed. In addition, BOP plans to evaluate the effectiveness of its outreach activities, for example, by monitoring access to the BOP and National Institute of Corrections (NIC) Internet sites to assess the effectiveness of this mechanism in reaching its targeted audience.
- On March 1, 1999, BOP sent a letter to all members of NIC informing corrections officials about possible Year 2000 problems beyond those related to computer software and hardware. It mentioned such matters as embedded microchips in equipment like metal detectors, X-ray machines, and elevators, and encouraged officials to look into the compliance of such equipment. The letter informed recipients about the BOP and NIC Internet sites and provided the addresses to reach them. It also provided phone numbers to call if the recipients needed further assistance. BOP plans two more follow-up mailings throughout the year that will provide updated information, as appropriate, to state and local correction officials.
- Also, BOP plans to make a limited number of follow-up phone calls to recipients of the letter. The calls will be used to assess the usefulness of the initial mailing, and depending on the findings, to modify future mailings to better meet needs of the state and local facilities. Second, the calls will ask whether state and local facilities need assistance in their remediation. BOP officials admit that they have limited ability to provide direct assistance, but they believe they can share lessons learned during the course of their own remediation work.

Other Justice Outreach Efforts

Following are descriptions of other outreach efforts being carried out by the Department of Justice:

- On December 11, 1998, the CIO chaired a Year 2000 outreach session with the Government Advisory Group for the Global Criminal Justice Information Network. Members of the Advisory Group include the American Correctional Association, the International Association of Chiefs of Police, the National Sheriffs Association, and the National Association of Attorney Generals, among others. The FBI made three presentations at the outreach session concerning the compliance of its key systems and forensic laboratories.

---

[5] "*The President's Council on Year 2000 Conversion: First Quarterly Summary of Assessment Information* (January 7, 1999).

[6] *Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts* (GAO/AIMD–99–23, January 27, 1999).

• On January 25, 1999, the Attorney General sent a letter to the presidents of seven law enforcement/criminal justice associations intended for publication in association newsletters. The letter discussed potential Year 2000 problems associated with law enforcement and the formation of the President's Council on Year 2000 Conversion. It also provided the address of the Council's Internet site and encouraged state and local law enforcement agencies to take a hard look at their buildings, computers, and other devices that could be susceptible to the Year 2000 problem.

• The FBI has engaged in a number of activities to educate state and local law enforcement officials about the status of the FBI's mission-critical systems. FBI officials have spoken at law enforcement conferences about their Year 2000 program primarily to discuss the status of key systems, such as the National Crime Information Center system, and to provide assurance that these systems will be unaffected by Year 2000 problems. The FBI has also recently published an article in several law enforcement publications [7] discussing the experiences the FBI had with its system remediation and encouraging state and local law enforcement groups to institute their own Year 2000 programs. The FBI is also using the Criminal Justice Information System Advisory Board, run by state representatives, to communicate Year 2000 information to state and local users of FBI systems.

• The Office of Justice Programs is working to build awareness through two forums. First, in July 1998, it distributed a notice to all grant recipients that all new equipment purchased with grant money is required to be Year 2000 compliant. The notice provided an Internet address and a phone number where recipients could obtain Year 2000 information. Second, at regional financial management training seminars held throughout the country, the Office has been working to build Year 2000 awareness by discussing some basic information about the problem.

• The Drug Enforcement Agency (DEA) has stated that the focus of its outreach efforts is making sure that its system interfaces with state and local and other counterparts are fully compliant. The DEA is also working with state and local law enforcement in field offices where DEA shares facilities with local or state counterparts.

In conclusion, Mr. Chairman, not enough is known about the status of either the 9–1–1 system or of state and local law enforcement activities to conclude about either's ability during the transition to the Year 2000 to meet the public safety and well-being needs of local communities across the nation. The Emergency Services and Telecommunications working groups have been active in this area and plan to follow up on their initial surveys. The Police/Public Safety/Law Enforcement/Criminal Justice working group has further to go to develop a more defined assessment but is moving forward.

However, more needs to be done than simply determining the status of these two critical sectors. More specifically, these sectors, under the leadership of the Council should use the information made available through the working group assessments to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

Mr. Chairman, that concludes my statement. I would be happy to respond to any questions you or the Committee members have.

RESPONSES OF JACK L. BROCK, JR. TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. In your testimony, you say that only 18 percent of the 4,300 9–1–1 call answering sites throughout the nation responded to a Federal Emergency Management Agency (FEMA) survey, and that of those 800 or so respondents, only 16 percent or a little over 100 reported their systems Y2K compliant. That is frightening! It means that most of the nation's 9–1–1 systems, i.e., over 4,000, are not compliant. And it does not raise our comfort level that, with a little over 8 months remaining before the date change, most assert that these complicated systems will be made compliant in time. Are these statistics as alarming as they appear? What assurances do we have that Americans will have uninterrupted 9–1–1 service after the century change? Can you offer any reasons first for the low survey response rate, and second for the dismal performance of this group? Do you agree that, in general, those with the best programs are more likely to respond to surveys and, if so, are these statistics even more dismal than they appear?

---

[7] *Law Enforcement News*, September 30, 1998, *Law Enforcement Technology*, August 1998, *The Police Chief*, March 1999.

Answer. The general lack of information increased our concern about which—if any—critical emergency communications and law enforcement systems may not be compliant in time. However, we testified that successfully completing a 9–1–1 call next January 1—and taking full advantage of all the features of enhanced 9–1–1 service—is dependent on two major factors for which some good information is available. First, the ability of the public switched telecommunications network to transmit the call and, second, the ability of the Public Safety Answering Points (PSAPs) to process the call.

With respect to the public switched network, the Telco Year 2000 Forum on Intra-Network Interoperability Testing, which is made up of local exchange carriers representing 90 percent of all access lines in the nation, recently conducted tests to determine whether the public switched network could carry calls in a Year 2000 environment. The tests were performed on 54 different configurations of central office equipment that included a majority of the network components used in North America. Only six Year 2000 problems were identified by the Telco Year 2000 Forum in over 1,900 test cases on these configurations, which involved 80 products from 20 different vendors. Assuming these tests were carried out effectively, their results provide some confidence that, if remediated, the public switched network should continue to function into the new millennium with no major service interruptions caused by Year 2000 dates. However, these tests did not focus specifically on 9–1–1 services and, as such, they did not test numerous "back end" systems that a PSAP might use, such as computer-aided dispatch systems, call logging systems, call recorders, and radios. PSAP operators are responsible for ensuring that these systems operate and interoperate properly after the date change.

The status of the ability of PSAP efforts to ensure that they can effectively process 9–1–1 calls has become more clear since our testimony. The Network Reliability and Interoperability Council (NRIC) reports that major local telephone companies have taken action to ensure that PSAP systems they provide to their customers have been remediated. And since the time of our testimony, FEMA and the Department of Justice have worked to increase the response rate to the public safety organization Year 2000 readiness survey conducted by FEMA and the National Emergency Number Association. As of June 30, 1999, of the over 2,200 sites responding, 37 percent reported that they were ready for the Year 2000. Another 55 percent of those responding reported they would be Year 2000 compliant in time for the millennium.

We have no information regarding FEMA's initial poor response rate.

Question 2. We understand that contingency planning for most emergency service providers will consist of direct answering and dissemination of 9–1–1 calls, i.e., without today's level of automation. It strikes me that many organizations may not have the manpower or corporate knowledge to field calls "the old way." Do you think this is a viable option for contingency planning? If not, what concerns would you have with this type of contingency plan, and can you suggest an alternative?

Answer. The business continuity and contingency planning process focuses on reducing the risk of Year 2000-induced business failures and on safeguarding an organization's ability to produce a minimum acceptable level of services in the event of failures of mission-critical information systems. Falling back to disseminating 9–1–1 calls without today's level of automation is a viable contingency plan, to which there is no feasible alternative, for the three 9–1–1 sites that we visited. Nevertheless, implementing contingency plans is not a risk-free proposition and requires careful preparation to ensure that core business processes are adequately supported. This preparation includes thoroughly testing the contingency plans, dedicating required resources to implement the plans, and training staff to fulfill their roles during contingency operations.

During our tours of 9–1–1 sites located in Arlington County and Fairfax County, Virginia, we were told that both sites use manual procedures when their computer assisted dispatch systems are not operating (such as during periods of scheduled maintenance or during unforeseen system outages). Similarly, during a more recent tour of the District of Columbia's Fire and Emergency Medical Services 9–1–1 site, we were told that the District of Columbia can operate using manual dispatching procedures and has recently practiced doing so. All three organizations recognize that operating without computer assistance lengthens service delivery times, but that performance remains within acceptable limits.

Question 3. You indicate in your testimony that outreach efforts by Justice have been targeted to raising awareness only, and have been largely ad hoc in nature. Did your review uncover any particular reasons why Justice's outreach efforts to the over 17,000 law enforcement organizations in this country have been so lacking? What if anything in your opinion should Justice do to step up its outreach activities?

Answer. The Department's outreach activities have been ad hoc in large part because Justice lacks a formal outreach program with stated goals and defined strategies for proactively reaching out to state and local law enforcement entities. With the exception of the Bureau of Prisons, Justice's component bureaus also lack formal outreach programs with goals and strategies. As discussed further in the following question, the FBI has taken actions recently to assess the capability of states to receive and send information through the National Crime Information Center (NCIC).

Since many of Justice's components have the same law enforcement counterparts at the state and local level, the department's efforts could be more effective if the department centrally defined and implemented a clear strategy, with measurable goals, objectives, and timeframes, and targeted activities that were assigned to specific bureaus and were aimed at expediting the Year 2000 efforts of late starters.

Question 4. As you indicate in your testimony, little is known about the status of state and local law enforcement agencies because no assessment surveys have been conducted. We understand that the law enforcement working group of the President's Y2K Council now plans to conduct such a survey. What recommendations would you make to maximize the timeliness and value of this survey? Considering that there is little over 8 months remaining until January 1, 2000, what should be done with the results of this survey? Would a survey even do any good at this late date?

Answer. According to the Acting Deputy Assistant Attorney General for Information Resources Management, the FBI recently completed a survey of the 50 states to assess their readiness to send and receive transactions with NCIC 2000 (the NCIC replacement system) and is in the process of summarizing the results. The FBI could use this information to target those state and local law enforcement agencies most at risk of not being Year 2000 compliant and develop appropriate strategies and contingency plans to respond to the risks.

Question 5. What do you believe are the biggest problems facing the emergency services sector at this stage?

Answer. At a nationwide series of workshops for state and local emergency services managers sponsored by FEMA, the main issues raised by participants were (1) developing and disseminating public information, (2) successfully completing contingency plans and Year 2000-related tests and exercises, (3) obtaining resources to address the Year 2000 problem, and (4) addressing concerns about human services including medical care, needs of special populations, and provisions of food and shelter.

Question 6. Considering the seemingly low level of preparedness in the emergency services sector, particularly with Y2K compliance of complicated 9–1–1 systems, do you think it is likely that all of these systems can be repaired on time?

Answer. Since we have not examined the remediation plans for the 9–1–1 systems in the sector, we are not in a position to assess the likelihood of their being ready on time. However, we recently collected data on the Year 2000 preparations underway in the nation's 21 most populous cities. Thirteen of the cities reported that their 9–1–1 systems are already Year 2000 compliant. Another five cities reported that their systems will be compliant by the end of September 1999. Two cities did not expect their 9–1–1 systems to be compliant until the fourth quarter of 1999. One city does not own or operate a 9–1–1 system.

Additionally, based on the results of FEMA and Justice survey work, the number of PSAPs reported to be compliant has increased, as well as the number of PSAPs indicating that they will be ready for the Year 2000.

Question 7. We understand that you recently toured one of the 9–1–1 centers in the area. Can you tell us about that?

Answer. On April 21, we visited the Emergency Communications Center (ECC) in Arlington County, Virginia. Arlington County leases its 9–1–1 systems from Bell Atlantic, which has stated that the leased equipments is Year 2000 compliant. This equipment includes a call recording system, a computer-aided dispatch system, and a radio communications system.

Arlington County's ECC is served by eight 9–1–1 communication lines provided by Bell Atlantic. To minimize the likelihood of outages due to communication disruptions (such as severed cables), the trunks do not all come to the ECC from a single Central Office; four trunks come from one Central Office and four trunks come from another. In the aggregate, these trunks represent the ECC's communications capacity to accommodate peak traffic loads. Arlington County also operates a scaled-down ECC located at an alternate location that functions as a back up in the event of a disaster at the primary ECC. In the event of primary site failure, staff would literally flip a switch to re-route calls to the alternate site.

The ECC Administrator described the 9–1–1 call process for a hypothetical emergency call placed from Centreville, Virginia. The call would not be directly routed

to the emergency response provider, but would instead travel to a service point operated by the local telephone company (in this example, operated by Bell Atlantic) located in either Baltimore, MD, or Philadelphia, PA. At this service point, a lookup is done in an Automatic Location Information (ALI) database.

The call is then routed from the ALI lookup to the PSAP responsible for dispatching an emergency response unit to the caller's location; this is referred to as "selective routing." At the PSAP, an operator's computer screen displays the following information: calling party address, community, state, etc. The operator verbally verifies the caller's address. If the address information is correct, the problem is coded, notes may be added, and an appropriate response is dispatched. If the information is not correct, the operator overrides the ALI information, inserts the correct problem location, codes the problem, and dispatches the appropriate response.

Arlington County has completed its Year 2000 assessment of the systems in use in their ECC and spent $60,000 to remediate non-compliant software used in its touch-screen radio consoles. A contingency plan is in place and manual backup procedures are used in the event of computer-aided dispatch system failures.

On April 27, we visited the Fairfax County Public Safety Communications Center in Annandale, Virginia. Fairfax County has been working on the Year 2000 issue in conjunction with its PSAP vendor for about 18 months. On April 15, 1999, Fairfax County conducted a Year 2000 test of its PSAP system. The test was run for 2 hours during an off-peak period, during which time all systems clocks were advanced. Based on the successful results of that test, Fairfax County officials expressed confidence that their PSAP systems are ready for the Year 2000. However, in the event of a service disruption, PSAP staff would revert to the use of manual processes to deliver service to the public.

We based our answers to these questions on interviews with Department of Justice and Federal Emergency Management Agency officials, analyses of 9–1–1 survey data, and our visits to PSAPs in Virginia and the District of Columbia. We conducted this work from April through July 1999 in accordance with generally accepted government auditing standards. We did not verify reported data or status information.

PREPARED STATEMENT OF JAMES N. BROWN

This committee, with a strong sense of focus and determination, has done an admirable job of confronting a virtually unparalleled challenge in the form of the Year 2000 "Millennium Bug" technology issue that carries with it an enormous responsibility, considering the global implications at stake. I am honored and privileged to come before you this morning to provide you with a municipal law enforcement administrator's perspective concerning Y2K and the contributing factors that have led to varying degrees of apathy from within the law enforcement profession which has not emphasized a strategic response in the form of a community-wide contingency planning objective.

As the Chief of Police for the city of Hudson, Ohio, a residential white collar professional community of approximately 23,000 residents within a 25 square mile geographical boundary between the cities of Cleveland and Akron, I have oftentimes, as have my colleagues, found myself having to contend with various problems that society has either chosen to ignore or has elected to categorize in broad terms as a "safety and security" matter. In the blink of an eye, our safety and security can be compromised by a terrible experience that was perhaps manageable or avoidable had we been attentive to the various indicators of an impending problem or crisis. Y2K presents classic indicators of such a nature that the law enforcement profession would be hard pressed to ignore.

Basic utility services alone are critical components of a community's safety and security. Although their dependability is remarkable, it has correspondingly lulled many of us into a false level of expectation whereby failure is an anomaly. This phenomenon is obviously not law enforcement specific, and there are certainly a number of communities nationwide who can readily attest to nearly insurmountable difficulties attributable to power outages and telecommunications failures, as can the law enforcement agencies who faced these challenges.

In the absence of active discussion at various association meetings, regional conferences, etc., the virtual non-existence of Y2K-related training sessions specifically designed for law enforcement, and a general lack of law enforcement specific web sites addressing Y2K from something other than a technology perspective, it is unlikely that most agencies have even discussed the potential ramifications that Y2K poses not only for their own operations but ultimately for the communities whom they serve. Conducting an inventory of critical IT (Information Technology) systems

for Year 2000 compliance is an important component of the Y2K situation, but a fractional one amidst a possible avalanche of problems.

I have found in my experience to date that most law enforcement administrators are genuinely concerned about the potential implications Y2K may generate and are sufficiently motivated to prepare their respective agencies and communities if they are afforded multiple training resources, informative documentation, and some basic guidance and direction from colleagues within our own profession. The law enforcement profession is equipped with vast media resources through its many associations, and yet, with few exceptions, there has not been much substantial in coming to terms with contingency planning. Thanks to the courage, wisdom, and vision of Kent State University, the Ohio Chiefs Association, and most recently the International Association of Chiefs of Police, I believe I may have finally succeeded at opening a few doors to an otherwise well-secured fortress.

There is a considerable level of apathy from within the profession concerning Y2K, and a variety of factors have influenced this response. There's considerable contradiction and rhetoric amidst the voluminous amounts of documentation being made publicly available which, I believe, has clouded the issue and drastically minimized Y2K's credibility as a potentially serious problem. Terminology such as "minimal impact" and "sporadic disruption" have created a comfort factor for those skeptics within my profession who, now more than ever, appear willing to role the dice and take their chances. Perhaps a dangerous game of Millennium roulette. "Sporadic" implies the existence of some distant community on the other side of the globe to which we have no allegiance or direct responsibility. The immensity of our communities oftentimes jades our sense of the enormity of the United States. The perspective changes rather dramatically when I suggest that a person approach a map of the United States armed with a straight pin and place the pin through the center of their hometown. I then pose the question: "Could your hometown be Sporadicville?" Perhaps it's the absence of the oftentimes overwhelming collateral structural damage and destruction normally associated with most natural and manmade disasters that has caused many law enforcement administrators to downplay the significance of Y2K. Responsible police administrators have absolutely no choice other than to plan for the worst-case scenario and hope, as you, for something significantly less. It would be unacceptable and irresponsible to do anything less. We have before us an opportunity and a challenge to transform our concern into a creative and effective action plan that will pay significant dividends to our communities whether Y2K-related problems come to pass or not.

Perhaps it's the absence of a sustained media campaign to bring the Y2K implications and possible ramifications to the attention of the American public, which to date has been sporadic. One of two local television reporters representing large networks who personally assumed an active interest in Y2K was advised by management that the issue was "too frightening" and might induce fear and cause people to panic. This from the same network that daily provides graphic pictorial details of human misery and death worldwide.

Several weeks ago, I forwarded a letter to the general managers of 12 different newspapers and radio and TV stations, along with some general Y2K information, advocating the necessity for additional media exposure. I received not so much as a single response suggesting that they had at least received the information, considered it, and decided against pursuing it further. When I wrote one of the more prolific nationwide law enforcement publications and provided them with significant amounts of "contingency planning" and "personal preparedness" documentation I have authored and felt would be beneficial for my colleagues, I was informed that the publication did not accept articles of a similar title. The article printed prior to my suggestion dealt strictly with IT issues. I expect an aggressive amount of media exposure in the final 8–12 weeks of 1999, which poses particular difficulties for law enforcement agencies who have failed to create a communications bridge with their residents concerning community-wide contingency planning and some basic guidance surrounding "personal preparedness." Quite frankly, we can most assuredly anticipate fear, panic, and a chaotic response from the public if we fail to educate our communities and dispel the Armageddon/ survivalist mentality, the prevalence of which will continue to grow disproportionately due to a lack of information from well-respected sources. The creative magic of communication carried out in a positive, informative, and well-intentioned, forthright manner will prove beneficial to the community, even if a worst-case scenario were to come to pass.

With the exception of a relatively small percentage of communities and law enforcement agencies throughout our country who have experienced calamity, managed it effectively, and are thoroughly prepared to implement a successful contingency plan at a moment's notice, there are all the rest who need to revisit their "dis-

aster planning" manuals or write a simplistic, yet functional one in earnest in the upcoming weeks/months, if one fails to exist.

Although there are indeed many agencies who do in fact possess a comprehensive disaster plan that would certainly address any difficulties Y2K may pose for their communities, these plans are also typically voluminous and sophisticated beyond practicality. Furthermore, even those plans that are simplistic in nature and capable of being readily implemented and sustained for varying durations can be complicated from an operational standpoint due to personnel limitations, equipment resource shortages due to strained budgets, and the general chaotic environment routinely experienced at the onset of any crisis. Most crises possess multiple personalities and a relentless, ever-changing, and dynamic penchant for sustaining themselves for seemingly prolonged durations until surrendering to a semblance of order and normalcy.

The perfect plan loses its luster and its brilliance if the true beneficiaries of its development and execution, our residents, are unaware as to how they summon critically needed emergency services in the absence of a functioning telecommunications network; the availability of predetermined shelters if they have exhausted their own resources, or their own homes are, and/or become, uninhabitable; and we have failed to provide simplistic yet essential guidelines as to how the average person or family can become self-sustainable in the absence of government assistance.

Most of us have fortunately never experienced a crisis of disastrous proportions, and yet that, unfortunately, breeds a false sense of security and complacency that can cause us to be caught off-guard if ill-prepared or unprepared. Law enforcement has typically had to manage every conceivable type of catastrophe at a moment's notice, and it has done so with a confident bravado and an envious swagger that are reassuring characteristics and attributes in the absence of order. We have exhibited a prevailing sense of "winging it," expecting a successful outcome with a bit of luck, a serious dose of common sense, and the on-scene dramatics of an effective leader challenged by the impossible. Continual reviews, updates, and modifications are maintenance issues of disaster manuals that are oftentimes tabled due to more pressing priorities. There is, however, no such thing as being too prepared or being so well schooled as an organization in disaster management or contingency planning that some level of attention cannot be devoted to tailoring some Y2K specific planning. It is anticipated that as law enforcement administrators continue to be educated and updated on the possible implications Y2K may pose for their organizations and the communities they serve, a much more aggressive contingency planning and personal preparedness campaign will be launched in earnest well in advance of December 31, 1999.

There are those people, law enforcement administrators included, who contend that the Y2K issue is all hype, is well on its way to being adequately addressed, and is nothing whatsoever to be concerned with.

Perhaps, and I hope they're correct! However, contingency planning and community preparedness will serve us all well, no matter what happens on January 1, 2,000—or any other date beyond 1/1/2000 for that matter. The character, grit, and determination of the law enforcement profession continually faced with challenge and adversity lend themselves to a successful outcome, regardless of the nature of the event. The local law enforcement agency is, in some respects, the first and last line of defense for our communities, and they will be looking at us, as law enforcement administrators, for direction and guidance as 1/1/2000 approaches. The law enforcement profession must recognize this responsibility and meet the challenges it presents. Be there no mistake about it, however; our dependability and reliability is, as always, rock solid, and with specific regard to Y2K, it's the lone absolute amidst a world of uncertainty.

Thank you.

RESPONSES OF JAMES N. BROWN TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Chief Brown, you testified that there is an absence of active discussion of Y2K preparedness at law enforcement association meetings and regional conferences, and that there are few Y2K-related training sessions for law enforcement. Who, in your view, has ultimate responsibility for ensuring that Y2K issues are addressed in such forums?

Answer. I believe that the editorial staffs of all the major law enforcement publications have a responsibility to address the Y2K issue from something other than an information technology perspective, i.e., contingency planning, disaster management, personal preparedness, etc.

In addition, each state chiefs' association likewise has a responsibility to encourage its membership to think along the lines of contingency planning, preparedness, etc., as do the various local county chiefs' associations.

Question 2. You testified that one reason for the level of apathy from within the law enforcement profession concerning Y2K is the contradictory information about the issue, as well as terminology that you believe creates a "comfort factor." Do you think there is any way that the law enforcement profession can wade through this contradictory information in order to conduct adequate preparations for Y2K emergencies?

Answer. Those within the profession are more apt to take direction and guidance from their colleagues also within the profession. There are very few of us out there attempting to deliver this message. The necessity for media cooperation through the various associations and their periodicals is critical. It is incumbent upon the state chiefs' associations, as well as the International Association of Chiefs of Police, to host a number of conferences to address the Y2K issue, with particular emphasis on contingency planning and personal preparedness.

Question 3. Chief Brown, you testified that you've had trouble getting the media to cover the Y2K issue because, in part, of the media's fear of causing panic. Do you think that it's possible for the media to find a balance between causing panic and providing responsible information to communities? If so, what is this balance?

Answer. Media professionals are unquestionably capable of providing responsible information to the communities. Finding a balance can, of course, be a difficult proposition because each reader interprets what he has seen or read from his own perspective. Actually, the media has an opportunity to promote contingency planning and personal preparedness for use in any disaster scenario by merely utilizing Y2K as the vehicle to deliver the message.

Question 4. Tell us about your own participation in Y2K awareness activities.

Answer. Personally I have spent well over a thousand hours of research on the subject, I have been involved in a number of public presentations for various communities and community groups, and I have been actively involved at the state level with training for law enforcement officials through the Ohio Chiefs Association. I have sent mailings to all county administrators, be they Mayors or City Managers, and have offered presentations for their staff members. As the President of the Summit County Chiefs Association, I have inundated my membership with information. Most recently, a web site was created by a member of the Hudson community for purposes of sharing my thoughts and views with other law enforcement agencies around the country, as well as with private individuals. The web site address is www.hudson-oh-pd.org.

Question 5. I understand that you contributed to the recent Project Impact initiative on Y2K which the International Association of Chiefs of Police sponsored. Can you tell us about this initiative?

Answer. I provided them with the documents that I authored concerning the Year 2000 issue and its impact on law enforcement. IACP's editorial staff then chose limited portions of my documents, as well as those of others who also provided information. I thought the initiative was well done; however, I also think each police agency should be on the receiving end of numerous other such mailings between now and the end of October.

Question 6. How would you assess the activities of the major law enforcement associations regarding Y2K?

Answer. I think I have previously addressed this subject; however, generally speaking, I think the coverage of the Y2K issue has been far too limited to the information technology difficulties that various agencies may experience. Y2K presents a unique opportunity for every law enforcement agency to address the issue of community-wide contingency planning.

Question 7. What are your greatest concerns regarding the impact of Y2K on local law enforcement?

Answer. I have addressed well over 500 police officers representing over 300 police agencies and have posed a simple question: How many of you have a plan in place to address emergency calls for service in the event the telecommunications network becomes disabled, for whatever reason, in your community? Two agencies out of 300 indicated they had a plan in place. I am extremely concerned that many mid-America law enforcement agencies who have fortunately not experienced a serious crisis or disaster are extremely ill-prepared to do so. Y2K planning will prove to be of significant benefit in any disaster scenario. Every agency speaks confidently of the existence of a disaster plan, and yet very few have ever worked with one. America's well being is dependent upon the reliability of local law enforcement. It is absolutely essential that every police administrator within every law enforcement agency from east coast to west coast recognize that responsibility. The preparedness/ contingency

plan need not be complicated or costly, but there MUST be a plan, and it has to be understood by every member of their organization and as many residents within their respective communities utilizing every available media outlet and community policing opportunity to convey that message.

PREPARED STATEMENT OF STEPHEN R. COLGATE

Good morning. I am Stephen R. Colgate, Assistant Attorney General for Administration, and the Chief Information Officer of the United States Department of Justice (DOJ). I am pleased to be able to share with you today some of my observations about Year 2000 (Y2K) readiness in the state and local law enforcement community. I hope you will appreciate that those observations are from the perspective of one who is not a member of the state and local community, and whose perspective is that of the Federal Government as a mission partner with different operational and resource considerations.

I would like to speak to the five subjects areas of your invitation from two separate viewpoints. First, I will address them from the viewpoint of the DOJ, then from the viewpoint of the working group that I lead under the President's Council for Year 2000 Conversion. That working group has a very broad scope that involves more than local and state police agencies, and includes law enforcement in the context of such Federal regulatory activities as clean water and safe food.

The DOJ has a mutually dependent relationship with state and local law enforcement agencies in many respects, including the temporary housing of Federal prisoners in local jails, the transfer of grant monies with the need to monitor and account for them, the collaboration in team-based criminal investigations, and the operation of large-scale, national telecommunications and information technology networks. We have as big a stake in smooth operational continuity at the year's end as do our non-Federal mission partners. Yet, it is important to note that those partners are extremely diverse and numerous, and not all of them are typically called "law enforcement agencies." For example, university departments of criminal justice that are grantees of our Office of Justice Programs are not necessarily included in the law enforcement agency category, and neither are the manufacturers, prescribers, and dispensers of controlled substances that file regulatory reports with our Drug Enforcement Agency. Yet, both are DOJ mission partners and both involve the flow of information that is potentially affected by Year 2000 problems. I could mention also the information activities of Immigration and Naturalization Service (INS) that involve mission partners that are not usually considered law enforcement agencies, but are most important to the INS and to DOJ.

DOJ bureaus and divisions are responsible for all aspects of their missions, including addressing mission partner readiness. I am pleased to tell you that they have been working extremely hard at this for a great many months, and are in a very good position to make as smooth a transition at year's end. We have been reporting our progress regularly to the Office of Management and Budget (OMB), which has been sharing it with the Congress, and we are continuing to do so along with the other Federal agencies. In addition, OMB has singled out three DOJ mission areas, Immigration, Federal prisons and the National Crime Information Center (NCIC), as "high impact Federal programs" requiring additional reporting.

Your invitation addressed specifically "the Y2K awareness of state and local law enforcement." I see this as having two principal dimensions. One is the awareness relative to their mission-partner interactions with DOJ. The other is awareness relative to the activities that are purely and entirely state and local, not involving the mission interactions with the Federal Government. Examples of the former include those I have mentioned above, plus the Federal Bureau of Investigation's (FBI) fingerprint processing, the FBI's forensic laboratory services, and the FBI's NCIC. Examples of the latter include city police enforcement of parking meters and regulations, and city police maintenance of safe vehicular traffic on city streets.

DOJ's strategy for Y2K awareness has been to concentrate on the operations in which we are a party. In so doing, we have encouraged our state and local mission partners to follow our lead and look to all of their own operations including those that do not involve the Federal Government. We are mindful that Y2K readiness starts with awareness, but if that awareness is not accompanied by the combination of timely and appropriate funding and the availability and employment of the necessary specialized technical skills, the awareness will yield nothing.

Over the past 10 months, DOJ has waged a campaign of Y2K awareness with its mission partners in all mission areas, and especially in law enforcement. That campaign has included the Attorney General, myself, component senior officials, operations and staff personnel who are on the front lines of telecommunications and in-

formation systems, and laboratory operations. The campaign has included Y2K messages in speeches to national law enforcement agency audiences such as the International Association of Chiefs of Police, letters to the heads of such national law enforcement associations as the National Sheriffs' Association and National Association of Police Organizations, presentations made to national mission partner audiences by the Department's Y2K program manager, and instructions and other materials sent to the thousands of Office of Justice Programs grantees.

I am pleased that Harlin McEwen of the FBI is here today to tell you some of the specific awareness activities that the FBI has been conducting. These have been so extensive that we have been getting some informal anecdotal feedback that many state and local officials have heard the message so loudly and so many times in so many venues that they can practically recite it from memory. There is no doubt in my mind that the FBI has done a stellar job of communicating Y2K awareness to all of its mission partners, which is all of the fifty states and United States Territories. They now know well the two things that are of paramount importance to DOJ, namely that DOJ is doing its own job of Y2K readiness so that the states can depend on DOJ's end of the partner relationship, and that they—the states—must do certain things to ensure that their end of the partner relationship will be Y2K ready. Those things include data exchanges that are part of information system operations, and are being tested as part of DOJ's overall Y2K readiness validation and verification processes.

I would like now to address your topics from the viewpoint of the leader of the working group for Police/Public Safety/Law Enforcement/Criminal Justice of the President's Council on Year 2000 Conversion. That group title is a mouthful that covers an extraordinarily wide spectrum of activities and entities. The activities include not only all that we usually associate with police, but all of the criminal justice enforcement dimensions of environmental laws and regulations, Federal lands and waterways management, and the public safety dimensions of mass transit systems and infrastructure. The entities include not only those that are part of state governments, but those that exist at county, city, and township levels. In the case of just police, the entities number into the tens of thousands, because almost all of the smallest villages and towns, like their big-city brethren, have their own police departments. Those departments may consist of just a chief and a deputy, but it's still a separate police department with dispatch and recordkeeping.

What is important to note for this "sector" of the nation, is that the smaller the police department, the more of them there are, and the more they rely on parties outside the Department for their information technology services and support. They look for their Y2K leadership and support to their municipal governmental structures and to their state capitols. To the extent that DOJ's Office of Justice Programs reaches down to the township level in grants administration, and our U.S. Marshals Service and INS work with local sheriffs on housing Federal prisoners or detainees in local jails, we have had the opportunity to interact at this smaller-entity level. As Mr. McEwen will indicate, the FBI's interactions are particularly strong at the state government level, and rely, for example, on state police entities to ensure that the NCIC links to the municipalities in the state, which are on state-operated networks, will transition smoothly to January 1, 2000.

As you may know, the working group includes several different Federal agencies. Two principal common elements are the enforcement of Federal statutes the violation of which carries criminal sanctions, or a mission-partner involvement with state and local law enforcement agencies. One working group member, the Postal Inspection Service, is in the group because of the first element, while the Federal Highway Administration is with us largely because of the second element. The greatest emphasis on state and local Y2K readiness has come from the agencies that have the most state and local mission partner interactions or are the most effected by what state and local agencies do. Let me give you a brief sketch of some of the more prominent endeavors.

In the case of the Federal Highway Administration, they recognize, as do we in DOJ that problems in traffic signal systems could tie up police officers until the problems are resolved. That could prove at least as troubling as the traffic disruption from an electrical outage. Because of the possible scope and impact of signal system malfunctions, such as confusing work days with a weekend days, the FHwA has been going to great lengths to advise city roads and highway administrators about possible problems with specific devices and systems, and strategies for their remediation. Of all of the working group participants other than DOJ, the FHwA has the most potential impact on state and local law enforcement even though those agencies are not its mission partners. They have been doing a thorough job of state and local agency awareness, but I have the impression that the critical issue now for state and local administrators is the size of the available pool of engineering ex-

pertise. If the demands on that pool exceed its capacity, some remediation efforts will be pushed beyond January 1, 2000, even though jurisdictions may have the funds available before the year-end.

Similarly, the Coast Guard and Interior Departments have been working extremely hard with their respective state and local mission partners to do more than just communicate Y2K awareness, but to interact with them to pursue actual readiness, as DOJ has been doing with its mission partners. In the case of the Coast Guard, the focus is on port operations and navigation systems. The Interior Department plays a major role in certain parts of the country and in certain states, such as Utah. Interior operates major dams and hydroelectric systems, road and communications systems, and other activities that fall under such components as the Bureau of Reclamation, Bureau of Land Management, and Bureau of Indian Affairs. Many of these involve embedded chips, which is why the Interior Department has created an office specifically to address the Y2K embedded chip issues for Interior-operated systems. I believe that the Interior Department has been working very hard on awareness and remediation, especially concerning embedded chips.

In recognition of the potential impact on law enforcement of problems with water and sanitation systems, the Environmental Protection Agency (EPA) was included in our working group. It enforces statutes involving criminal sanctions, as well as operates mission-partner activities with all of the states. The EPA has been particularly concerned with the avoidance of major Y2K anomalies not only in water and sanitation systems, but also in industrial chemical discharges into the air or water. I believe that EPA has done a magnificent job of Y2K awareness with its state and local mission partners, and has been addressing regulatory provisions that can stimulate Y2K readiness by industrial operations that fall under its discharge reporting regimens.

In a similar vein, the Agriculture Department's Food Safety and Inspection Service (FSIS) has an enforcement mission that recently joined our working group. Should problems arise with food supplies, like water supplies, state and local law enforcement agencies might be called upon to provide protective services at warehouses or retail outlets. In an effort to obviate this, the FSIS has been pursuing a systematic Y2K food industry readiness campaign, starting with the largest corporations and working down the size pyramid to the smaller suppliers and outlets.

Additionally, our working group has had the earnest participation of the Department of Defense (DOD), and I am deeply appreciative of the DOD's support. In the Y2K context, I view DOD in two ways. First, DOD operates many facilities in the U.S. with weapons systems that employ computers. Should something go wrong with any DOD weapon, manufacturing, or discharge system on or just after January 1, 2000, it is conceivable that law enforcement agencies might have to assign resources to deal with the event. On the positive side, National Guard organizations represent an immediately available pool of trained personnel who can be tapped to assist state and local law enforcement should such assistance be needed. If the situation warrants, Active and Reserve forces could also be brought to bear. I do not anticipate such need, but it is comforting to know that our nation has these resources.

Your invitation asked also that I speak to assessment, readiness concerns, and recommendations.

In light of what I have described above for the Police/Public Safety/Law Enforcement/Criminal Justice Working Group, any efforts toward assessment need to be more narrowly drawn, so as to focus on aspects that are reasonably homogeneous in mission and size. In this context, I would like to speak specifically to law enforcement, as comprising state and local agencies staffed with sworn officers having the power of arrest.

As I noted above, just these entities number into the tens of thousands when one includes all the tiny departments in towns and villages, all the sheriffs, and all the entities with police powers that aren't responding to domestic calls, such as transit police and park police. Most of these entities receive all of their funding from local or state legislative bodies. Perhaps even more significant, most receive all or the bulk of their computer support from sister agencies in their local or state governments that provide computer services and support and that possess computer expertise. Very few small law enforcement entities have their own computer expertise. Many do not even operate their own dispatch systems, but share dispatch operations with local fire and ambulance services.

We have made available our assistance to independent, non-governmental entities in which local governments participate, in the formulation of their own Y2K support endeavors. Those endeavors include the development of guidance publications, such as issued recently by the International Association of Chiefs of Police, and assess-

ment surveys such as the one about to be conducted by the National Association of Counties.

Quite apart from the formal assessment activities of surveys, we get feedback of an informal and anecdotal nature from our mission partners in the conduct of our mission activities. Because the FBI has the most such interactions, I will let Harlan McEwen share with you their sense of where things stand with their mission partners. In general, the assessment picture appears to be one where there is now widespread awareness in the law enforcement community of what the Y2K problem is and what needs to be done, generally, to remedy it. In the larger metropolitan agencies and at the state government level, there is usually an in-house capability to identify and remediate Y2K vulnerabilities. In the smaller agencies, that identification and remediation must come largely or sometimes entirely from sister entities that have computer budgets and expertise, and that usually provide computer services to multiple governmental activities.

It is my view that when one looks at municipal law enforcement agencies, apart from the Federal and state interactions that I have addressed above, one sees basically three activities. The first and most important is a presence on city streets and neighborhoods. Generally speaking, that comes down to automobiles with gas in their tanks and officers reporting for duty. The word about Y2K has gotten out sufficiently that most agencies will have their officers all available for duty if not actually reporting for duty on January 1, 2000.

The second activity is communications. This involves the dual aspects of radio dispatch and the ability of mobile units to operate with their dispatchers. Unfortunately, it is in this area that the embedded chip issue most affects local law enforcement. You have already heard from various sources about the issue of embedded chips, which affects much more than just communications devices. I wish I could give you assurances that all law enforcement agencies of all sizes will have on December 31 dispatch systems and mobile radio unit devices that are Y2K "certified" by their manufacturers. The good news is that many of these systems and devices that are not so certified will nevertheless operate satisfactorily. Within DOJ, we have given careful attention to our own land mobile radio systems to ensure their Y2K readiness.

The third activity of local law enforcement entities that has Y2K vulnerabilities is recordkeeping. This is the activity area most associated with Y2K and computers. The Y2K problem is usually couched in terms of date computations in the context of records, such as the age of a person, or the expiration of a warrant, or the determination of a date for release of a convict from jail. It is for these recordkeeping activities that small law enforcement agencies rely most on services and support from outside their own agencies. Even in those agencies where a recordkeeping system resides in a desktop computer inside the agency office, the design and programming of the system as well as its maintenance has probably been done by someone not on the agency payroll. The design, programming, and maintenance have probably been coming from either a governmental counterpart to the Federal General Services Administration or from non-government contractors. The Y2K remediation of these recordkeeping systems is almost always a matter of funding, and the funds are entirely local or state or a combination of state and local. I am hopeful that the National Association of Counties survey that we understand is soon to be taken will give us all some insights into this activity area and confirm our belief that law enforcement and public safety sector is sufficiently addressing Y2K readiness.

Regarding your fourth question, about specific concerns the Department or the working group has regarding the Y2K readiness of state and local law enforcement, I would like to offer a few observations. In particular, I am somewhat concerned about the possibility that state and local law enforcement agencies may be called upon to deal with Y2K-related problems that may fall outside their sphere of professional preparation. As we all know, when a cat gets stuck in a tree or a rabid animal is seen in a neighborhood, the police get the call for help. Law enforcement agencies are viewed by the public as a first line of defense and protection against almost anything that is perceived as dangerous or upsetting. The police can't possibly anticipate everything that the Y2K bug may bring to their communities that will produce a call from a distraught citizen, but they will be willing and able to handle the many challenges brought to them.

To summarize, what state and local law enforcement will need on January 1, 2000, are highly visible uniformed officers with Year 2000 compliant radios. That date may bring a need for more men and women than are on an agency's payroll, particularly if they have to perform significantly more time-consuming tasks such as traffic management, in which case state and local governments may wish to consider using auxiliary or reserve personnel, including retirees still in the local area.

This brings me to your final question seeking recommendations for Congressional or governmental actions that might have a positive impact for state and local law enforcement. I believe that the Congress has been pursuing important actions in providing maximum incentives for the manufacturers of communications devices and systems with embedded chips to make full disclosure of their products' Y2K vulnerabilities. Nothing will affect law enforcement more than problems with radio dispatch operations, traffic signal systems, or with devices such as building security systems. Next to these, and the possible effects of such unusual major events as a chemical manufacturing plant malfunction, the computer-based law enforcement recordkeeping systems are relatively minor by comparison.

Thank you for this opportunity to share with you my observations on the Y2K readiness of state and local law enforcement. I welcome your questions.

RESPONSES OF STEPHEN R. COLGATE TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. You mentioned in your testimony that at this point the awareness level about Y2K in local law enforcement appears to be fairly high. That being said, what impediments to Y2K preparedness remain for local law enforcement?

Answer. We have no concrete reason to believe that there are impediments of such magnitude as to cause national concern. We believe that such impediments as may be found are (1) funding limitations and (2) the available supply of trained technical human expertise. We have been working closely with our state and local mission partners for many months, in all states, and these impediments are the only two that have been mentioned. They have not been mentioned universally—only occasionally.

Question 2. You mention in your testimony the extensive contact that the Justice Department has with its state and local partners in the law enforcement area. Has funding for Y2K been an issue for local agencies? Have there been many requests for federal funding from the local law enforcement agencies for Y2K?

Answer. As noted above, funding has been mentioned anecdotally and in the context of informal interactions. However, we have seen no formal requests for federal funding.

Question 3. One of the reasons we invited you here today is the Committee's concern about the absence of any substantive assessment information on the status of local law enforcement in the quarterly assessment report of the Year 2000 Conversion Council. What will be done to remedy this?

Answer. We are attaching to this set of questions and answers the full text of the assessment report that we sent to the Council for its July Quarterly report. We believe that it contains much substantive information. We understand the Committee's concern, and trust that this assessment report will alleviate that concern.

Question 4. Your testimony highlights a good level of activity on the part of the Justice Department to reach its partners. What we really need to hear about is what is being said at the other end of this equation. How can the comments and concerns of the state and local agencies best be captured and conveyed back to us?

Answer. We will continue to send to the President's Council our formal periodic assessment reports, which we understand are shared with the Committee, and related reports such as our quarterly readiness reports and our reporting on high-impact areas such as the FBI's National Crime Information Center. Additionally, we keep the Council's Chair, John Koskinen, apprised of significant items that come to our attention from activities such as end-to-end systems testing with local entities. The local concerns we have heard thus far deal with matters that are between local law enforcement agencies and the local governments of which they are a part and that provide their resources. I believe that such comments and concerns can best be captured and conveyed by parties with a state and local focus, such as the professional and state/local associations, e.g., the International Association of Chiefs of Police, and the U.S. Conference of Mayors.

Question 5. While your statement indicates that a fair amount of activity on Y2K has occurred in the law enforcement area nationwide, there appears to have been no attempt to analyze the impact these activities have had, nor to provide any road map regarding the remaining problems or firm indications of who else needs to be helped. How can we remedy this?

Answer. It is unfortunate that our assessment reporting to date has given the impression of lack of analysis, road map, or indications of needed help. We hope that our July Assessment Report, attached, will show that considerable analysis has indeed been done. As the report notes, we are about to engage in the end-to-end testing of systems that reach well into local agencies. We anticipate learning very much

in that process. Our goal is that it will be a smooth, reassuring experience, and we anticipate reporting our findings in the next quarterly assessment report. We will be encouraging other Federal Government agencies with systems interactions at the local law enforcement level to pay similar attention to their findings and the reporting of those findings.

Question 6. We appreciate the fact that local law enforcement is indeed a huge sector, but it certainly is no larger than that of the small business sector of our economy, and surveys have successfully been done in that area. Have you devised a strategy for at least conducting some type of limited survey?

Answer. We believe that no survey can reveal as much as is revealed in the process of the end-to-end testing of operational systems. That process includes all mission partners, the selection of a representative sample, and then the in-depth interaction with the selected entities that comprise the sample. Just as the DOJ has been conducting end-to-end testing of its systems, so will the other Federal Government agencies with whom local entities interact. A recommended strategy would be to focus on the compilation and reporting of what is learned in end-to-end systems testing. I will be addressing this within the Sector Working Group that I chair.

Question 7. In general, across most industries, professional associations have been the workhorses in Y2K preparedness in many ways. How would you rate the responsiveness of the professional law enforcement associations on the Y2K issue?

Answer. We have been most pleased with their responsiveness. We especially direct the Committee's attention to the work of the International Association of Chiefs of Police, and the fine document that is posted on the association's World Wide Web site. We note that this association has a larger full-time staff than many other associations in the law enforcement community, and has more resources to devote to the issue. When viewed in the context of their resources and the mix of issues that they are confronting, we are gratified by the responsiveness on Y2K of all of the associations with which we have dealt.

PREPARED STATEMENT OF VICE CHAIRMAN CHRISTOPHER J. DODD

911 is the national life line that allows Americans to reach out for help from wherever they are. Americans use 911 more than 300,000 times every day to access emergency services, law enforcement and medical services. While we all recognize the contribution that 911 systems make to public safety, few of us recognize how advanced the technology underpinning these systems have become. Dialing 911 gets a caller to a Public Safety Answering Point (PSAP). When that 911 call comes in to the PSAP, the phone number and location of the caller is transferred from special location databases and displayed at a computer console where an attendant verifies the accuracy. Each 911 call that reaches a PSAP is handled according to its location and nature. Typically, calls are then referred to law enforcement, emergency medical services, or local fire departments. The telecommunications industry has gone to great lengths to assure that 911 calls will not be disrupted by Y2K related problems. But the telephone companies can only ensure delivery of the calls to the PSAPs.

However, I would like to point out that we potentially have a very serious problem on our hands. The Y2K readiness of America's Public Service Answering Points may be in jeopardy. Recent survey information from the United States Fire Administration found that approximately 16% of the nation's PSAPS were ready. The Fire Administration surveyed over 4300 PSAPs and received answers from only 766 PSAPs. So, we have no idea how prepared 3534 critical answering points are for Y2K. Of the less than 20% of the answering points that responded 16% say they are ready. If these systems are not repaired they will increase response time and present a grave risk to the public.

Of the surveys they did receive, the Fire Administration was surprised to learn that only 40% of the responding organizations had a contingency plan. I quite frankly am a little surprised that such a critical link in the emergency response chain would not have contingency plans. I have had a chance to review some of these survey responses. The respondents consistently cite a lack of leadership, lack of funding, concerns about interdependency and the failure of vendors to supply compliance information.

Y2K failures in public safety answering points have the potential to hinder police and emergency responders from protecting our families. We cannot allow a lack of awareness about Y2K or a lack funding to compromise public safety. We need to find out exactly what the readiness problem is with the public safety answering points. One possible problem is that PSAPs are not regulated by anyone and there

is no single entity charged with coordinating a nationwide assessment and prompting remediation.

The lack of 911 readiness may be symptomatic of larger problems in law enforcement. When the President's Council released its second quarterly assessment on April 21st there was no assessment of law enforcement. We hope that this hearing will help "turn up the heat" as one might say in police jargon, and to encourage more activity in this area. I look forward to learning how the Department of Justice will reach out to the law enforcement community and help them address Y2K.

I am pleased to have Commissioner Michael Powell with us today. Commissioner Powell you have been doing excellent work on this issue. I understand that you will be presenting some updated information regarding PSAP readiness. I look forward to getting an update on these numbers. Commissioner Powell, the Chairman and I have written you a letter asking for help. While neither agency currently has any regulatory authority over the PSAPs, the Committee believes that a collaborative FCC and US Fire Administration effort could provide the critical leverage needed to reach this community. In fact together the FCC and the Fire Administration can hand the state Y2K coordinators or emergency managers a list of possible problem PSAPs. This will provide the states a valuable tool to ensure that the public does not suffer in any tangible negative effects because of Y2K.

I also want to welcome Chief John S. Karangekis of Wethersfield, Connecticut. Chief Karangekis is president of the Connecticut Police Chiefs Association and will give the Committee specific insight into the challenges local law enforcement face in arresting Y2K problems.

PREPARED STATEMENT OF JOHN S. KARANGEKIS

OVERVIEW

Informal survey of a cross section of police agencies in the State of Connecticut reveals that agencies vary in their level of progress to remediate Y2K issues prior to the turn of the century. There is consensus that it is imperative that each law enforcement agency show due diligence in their efforts to mitigate any adverse impact resulting from non-compliant technology. It is believed that the Connecticut experience is likely similar to that of other law enforcement agencies throughout the country.

The majority of large cities and towns in Connecticut appear to be ahead of some smaller communities in addressing the issues. It is clear however that all law enforcement agencies recognize the importance of due diligence and are actively addressing those issues in their own communities. A recently released Y2K Readiness Report distributed by the State of Connecticut, Department of Information Technology, regarding Y2K remediation efforts, gave strong indicators that only minimal adverse impact is expected. Utilities, water systems, petroleum and natural gas providers surveyed indicate that their services are either currently Y2K compliant or will be December 1999. The majority of those services will have contingency plans before the end of 1999. Most significantly, it appears that telephone service, E911 and other law enforcement technologies will be operational.

Like many communities, Weathersfield has initiated a town-wide Year 2000 Readiness Committee consisting of representatives from each town department or division. Individual departments determine Y2K compliance and remediation needs in their own department. Technologies that network with or interface in-house or with other town departments, or technologies that network or interface with outside agencies at the state or federal level, are identified and evaluated for compliance. At the present time, approximately 80% of all town and police technology, including computers, telecommunications, alarm systems, internal data systems and records systems are Y2K compliant. Progress is being made through follow-up, software upgrades, and/or replacement. Due to delays, ascribed to vendors' reluctance to provide clear information regarding their products, some technology has yet to be classified.

CONTINGENCY PLANNING

Regardless of perceived level of Y2K compliance, it is imperative that law enforcement have in place adequate contingency plans to address failures that may occur. During the initial Year 2000 turnover sufficient safeguards must be in place to insure public safety and the orderly maintenance of government. The delivery of services must not be significantly compromised during the turnover in the event that some failures occur.

It is the consensus of public safety officials that the majority of their technology will be Y2K compliant prior to the Year 2000. The first 72 hours of the rollover will be the defining test period. Minimal technological failures will not significantly im-

pact the ability of law enforcement to maintain order or respond to the needs of the community.

LAW ENFORCEMENT CONCERNS

1. The failure or delay in gaining specific information from various vendors as to the Y2K status of their equipment.

2. Reluctance of vendors to guarantee Y2K compliance.

3. Possible panic reaction by community residents prior to the 2000 turnover.

4. Significant costs associated with contingency planning, staffing and costs of updating hardware and software.

5. Developing emergency funding resolutions through grants.

INFORMATION RESOURCE

The International Association of Chiefs of Police recently conducted a survey of their membership relative to the Year 2000 readiness of law enforcement. The study resulted in the compilation of a 27 page document that has proven to be an invaluable resource for addressing Y2K public safety issues. The document is available on the IACP Web Page (*www.theiacp.org*).

PREPARED STATEMENT OF HARLIN R. MCEWEN

Good Morning. I am Harlin R. McEwen, Deputy Assistance Director, Criminal Justice Information Services Division, of the Federal Bureau of Investigation (FBI). I am pleased to have this opportunity to inform you of the work we have been doing at the FBI as it relates to assisting state and local law enforcement on the topic of Year 2000 (Y2K) readiness in their Criminal Justice Information Systems.

As a former city police chief of over 20 years, and as Chairman of the Communications & Technology Committee of the International Association of Chiefs of Police (IACP), I have been personally involved in educating and assisting state and local law enforcement agencies on Year 2000 matters for the past four to five years.

At the FBI we have taken a very proactive role in keeping the Y2K issue before the state and encouraging them to plan for and institute changes to make their systems compliant with our nationwide systems. In the FBI Advisory Policy Process, our primary interaction is with the 50 State Control Agencies (CTA) who are responsible for providing the appropriate interconnect with the FBI Systems and for providing the necessary statewide systems and access for state and local agencies to the FBI Systems.

The following is a chronology of the actions by the FBI to assess the readiness of the state CTAs and to insure they were aware of the consequences if state systems are not ready for the data change.

Spring, 1996

The FBI Criminal Justice Information Services (CJIS) Division prepared a staff paper for the Advisory Policy Board (APB) Working Group meetings presenting the Y2K issue and proposing alternatives for compliance. The Working Group recommended converting all dates in the NCIC System to the Y2K format. This recommendation was approved by the APB at the June, 1996 meeting.

September, 1997

The FBI CJIS Division and the Information Resources Division (IRD) hosted over 400 state and local criminal justice agency representatives at the NCIC 2000 Technical Conference in Tulsa, Oklahoma. At this Conference the timetable and formats for the Y2K data were presented and the need to plan for necessary changes was stressed.

September 25, 1997

The FBI CJIS Division sent a Technical and Operational Update to the states informing them of the timetable and formats for the data changes.

January, 1998

The FBI CJIS Division surveyed the states and requested information regarding the readiness of the states for NCIC 2000 and Y2K compliance.

July, 1998

At the request of the CJIS Advisory Policy Board, the states were sent a letter explaining the Y2K schedule and the consequences of not being compliant with the nationwide systems by July, 1999. The letter enclosed a form requesting the agency head sign a statement acknowledging that the schedule and consequences are understood. All states responded with a signed statement. The District of Columbia did not respond.

December, 1998

The District of Columbia Metropolitan Police Department contacted the FBI CJIS Division and indicated they were having difficulty with Y2K compliance and requested FBI assistance. The FBI CJIS Division and Information Resources Division responded to the District with technical consultants and the conversion software developed by the FBI to convert NCIC dates. Subsequent to this, the city government provided the department with resources and we have been assured that the situation is under control. This is particularly critical because the District of Columbia Metropolitan Police Department provides the interface to the FBI Systems for all law enforcement agencies in the District. This includes all DOJ components such as the FBI, the Drug Enforcement Administration (DEA), the US Marshals Service, the Immigration and Naturalization Service, and the Bureau of Prisons (BOP). It also includes the Treasury Law Enforcement agencies such as the US Secret Service, Bureau of Alcohol, Tobacco and Firearms (BATF), US Customs, and other agencies like the US Park Police and the US Postal Inspectors.

November, 1998—April 1999

The FBI CJIS Division and IRD have been conducting External Interface Checkout (EIC) testing with all states. The states have been strongly encouraged to use Y2K compliant data formats in these tests. However, it has not been mandatory as some states are still in the process of converting their software or have contracts with work in progress to make their systems Y2K compliant.

February, 1999

The FBI CJIS Division hosted over 400 state and local criminal justice agency representatives at the Integrated Automated Fingerprint Identification System (IAFIS) Technical Conference in Los Angeles, California. At this Conference the timetable and other issues related to Y2K issues were presented and the need to plan for necessary changes was stressed.

February—May, 1999

The CJIS Division and IRD are conducting Site Operational Tests (SOT). Those states which did not use Y2K compliant date formats in EIC are required to do so in SOT.

July, 1999

NCIC 2000 and IAFIS are scheduled to be fully operational, Y2K date formats are mandatory.

The FBI is prepared to offer assistance to a state that indicates they are having difficulty with Y2K compliance. We have encouraged them to come to us if they have problems. The response will be dictated by the circumstances, the particular needs of the state involved and the resources available at the time. We have been advised that all states are following a plan of action to get their systems compliant. However, as in all endeavors, they must succeed in that plan in order to avoid the consequences of noncompliance. Such consequences range from loss of some services to complete system failure. While some states have a very close time schedule, the only agency to have contacted the FBI and requested direct assistance has been the District of Columbia.

Thank you for this opportunity to inform you of the work the FBI has been doing to assist state and local law enforcement in getting ready for Y2K. I welcome any questions.

RESPONSES OF HARLIN R. MCEWEN TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. You testified that as Chairman of the Communications and Technology Committee of the International Association of Chiefs of Police (IACP) that you have personally been involved in educating and assisting state and local law enforcement agencies on Y2K matters for the past four to five years. That is extremely commendable. What significant outreach activities has the IACP performed during this period? What have been the critical areas you have found that required education and assistance? What remains to be done?

Answer. The IACP has been active in educating the law enforcement community on Y2K issues. The IACP has prepared a brochure entitled "PREPARING LAW ENFORCRMENT FOR Y2K". The IACP has widely disseminated this brochure to Police Chiefs and other law enforcement officials throughout the country. The IACP has also conducted workshops at the Annual Conferences, published Y2K related articles in "The Police Chief Magazine" and arranged for presentations on Y2K at various Committee Meetings. The most critical areas of discussion from participants has been the "*unknown*" in what are generally very complex communications systems. Many Police Chiefs report they are not able to reasonably assess or identify the potential problems and therefore it is difficult to attempt to solve them. At this

late stage, the IACP approach has been to recommend contingency plans in the event of system failures.

Question 2. A great deal of information is known about the readiness of those information systems and support services systems managed by the FBI, for which state and local government are primary "customers." What centralized assessments have been made of individual systems managed directly by local law enforcement agencies? Many of these systems connect to federal and state criminal information systems in various ways, what is known about these interconnections? What plans are there to perform end-to-end testing of these systems and their connections?

Answer. As I explained in my testimony to the Committee, the FBI manages the national systems on behalf of state, local, and federal law enforcement and must depend upon a single point of contact in each state and in the federal systems. We rely upon the states to administer the statewide networks which connect to the FBI national systems and the FBI does not have the resources to deal directly with the over 17,000 law enforcement agencies nationwide. On Sunday, July 11, 1999, the FBI activated the new NCIC 2000 systems which required that the states be Y2K compliant to work with the new NCIC 2000 protocols. With some minor exceptions the new NCIC 2000 system is performing to expectations and all states are communicating with the new system. In preparing for actual Y2K many states have been pro-active in conducting statewide user conferences and in surveying local agencies in order to inform them of potential problems, assess their situation, and assist in solutions where possible.

Question 3. The FBI is responsible for administration of the National Crime Information Center and has assured Committee Staff that this system will be fully able to meet its Y2K challenge, and that its links to the systems of all 50 states will remain fully operational. What type of independent verifications and validation has been done in this area? What plans are there for end-to-end testing of this system to ensure its operational capability? Given the criticality of this system, what type of continuity of operations and contingency planning has been done?

Answer. Please refer to the Answer to Question #2. A contingency plan was prepared by the FBI in preparation for the activation of the NCIC 2000 system on July 11th and FBI plans to use the same basic contingency plan for Y2K problems at year 2000 start.

Question 4. You noted the proactive role the FBI has played in encouraging states to plan for Y2K and make necessary changes to their systems. How receptive have the states been to the FBI in this role? What changes have you encouraged them to make? In your estimation, how have the states been in completing, implementing, and testing these changes?

Answer. Most of the states have been very receptive and cooperative. The states have been very responsive in completing, implementing and testing recommended changes.

Question 5. What are the consequences if state control agencies' (CTAs) systems are not ready for Y2K?

Answer. Loss of service. Although we are hopeful that will not happen, we have a contingency plan in place to handle, in the most appropriate manner, the specific state problem.

Question 6. You noted that the FBI stands ready to assist states that indicate they are having difficulty with Y2K compliance and have encouraged them to come to you if they have problems. The District of Columbia has requested direct assistance. What type of response have you had from the states in this regard? Do you anticipate any particular assistance requests that will require additional resources?

Answer. The response from the states has been very good. There may be some additional requests for assistance during the remainder of 1999 and if the FBI receives any we will respond accordingly.

Question 7. You have been advised that all states are following a plan of action to get their systems compliant with a very close time schedule. Is the FBI tracking progress of the states in some manner? Could you briefly explain? Do these action plans include business continuity and contingency planning in addition to independent verification and validation (IV&V)?

Answer. We are tracking the progress of the states and as I reported in my testimony we have conducted a state by state visit to get updated information and offer assistance where appropriate. This survey was conducted on a voluntary basis and with the understanding that we had no role in reporting state readiness to the public. This allowed for candid response and allowed us to be of assistance. It should also be noted that this survey is considered a "snapshot in time" and we have already seen significant progress in the efforts of those states requiring attention. As noted in my answer to Question #2 we have already activated the FBI NCIC 2000

system on July 11th and that gives us further assurance that the states will be ready for Y2K. Following is a summary of the results of that survey:

State Readiness Summary - June 1999

Issue	Fully Prepared	Requires Some Attention	Not Prepared
CTA Operations Beyond Y2K & NCIC 2000	44	7	1
Local Agencies' Systems	12	27	13

PREPARED STATEMENT OF MICHAEL K. POWELL

Thank you for the opportunity to be here today. As you are well aware, emergency services are crucial to the life and safety of Americans, and the Year 2000 (Y2K) Problem poses a real and palpable threat to the continued operation of these services. Unless providers of these services take appropriate steps to identify and remediate Y2K related problems within every facet of the emergency response process, Americans are likely to experience delays and perhaps even a failure of emergency response.

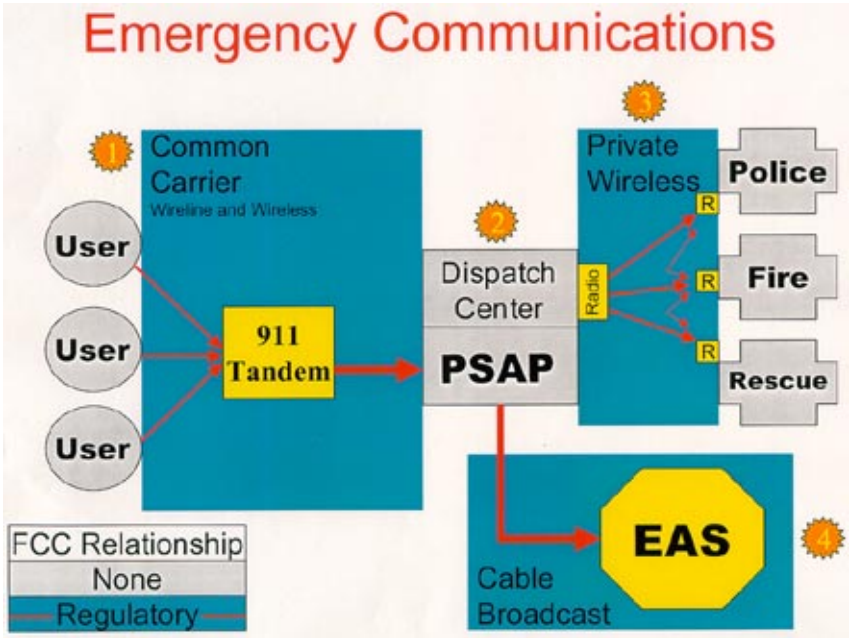
At the FCC we recognize that emergency communications are crucial to the emergency response process. For over a year now we have had an aggressive campaign aimed at identifying the risks posed to these systems by Y2K and raising awareness of the potential problems with those entities that provide emergency services. Forums, speeches, and articles are just a few of the ways in which we have reached out, and continue to reach out, to this community.

THE EMERGENCY COMMUNICATIONS SYSTEM

Before elaborating on our efforts and the assessment of this sector, I would like to take a moment to describe for you the emergency communications system. There are four main components to emergency communications: 1) 911 call delivery; 2) call processing at the Public Safety Answering Point (PSAP); 3) wireless call dispatch; and 4) the Emergency Alert System (EAS).

These four components are not part of a unified national system. Rather, there is extensive variation among the nation's counties, cities and towns in terms of the number, function and sophistication of the communications system employed. And any one system typically involves any number of components, each with a different set of vendors and suppliers, and each with potentially different regulatory or jurisdictional oversight. Yet, inasmuch as the system is comprised of a variety of systems, these systems must interoperate in order to achieve a successful response to an emergency.

The figure on the following page demonstrates this graphically.



There are approximately 300,000 emergency calls per day in the United States. The 911 Emergency Reporting System is the portion of the emergency communications system that enables a caller to dial a common three-digit number for all emergency services. Today, some form of 911 covers over 90 percent of the population.

Enhanced 911 (E911) is an advanced form of the basic 911 service. With both wireless and wireline E911, the telephone number of the caller as well as other stored information about the location of the caller is transmitted to the Public Safety Answering Point (PSAP) where it is cross-referenced with an address database to automatically determine the caller's location. The emergency dispatcher can then use this information to direct public safety personnel responding to the emergency.

1. *911 Call Delivery*

The first step in an emergency communication involves delivering the call from the person reporting the emergency to the appropriate dispatch center as indicated by the Number 1 on the figure. 911 call delivery is a traditional telecommunications service provided by the local telephone company. Remediation and testing of the switching and transmission equipment used in 911 service is part of the overall remediation efforts currently underway by the telephone companies. It is important to note that unlike other segments of the emergency communications process, the FCC has direct authority over the companies that route this initial call.

2. *Call Processing at the PSAP*

The second step typically involves processing of the emergency call at the PSAP as indicated on the figure by the Number 2. This step primarily involves computer processing and often employs sophisticated systems and software. At the PSAP, the operator verifies or obtains the caller's location, determines the nature of the emergency, and decides which emergency response teams should be notified. In most cases, the caller is then conferenced or transferred to a secondary PSAP from which help will be dispatched. Secondary PSAPs might be located at fire dispatch offices, municipal police headquarters, or ambulance dispatch centers. Often, a single primary PSAP will answer for an entire region. Communities without PSAPs rely on public safety emergency operators and communications centers to process these calls.

The PSAP, either primary or secondary, is especially vulnerable to Year 2000 problems because it generally relies on sophisticated computer technology and then interconnects many private networks with different types of equipment. As mentioned previously, there is no single configuration for emergency communications, nor is there a uniform entity responsible for maintaining the system across the nation, or even within a particular state. Thus, unlike the routing of 911 calls to the

PSAP, which is under the control of the local telephone company, the processing of the call at the PSAP is controlled by a myriad of different entities, none of which have a regulatory tie to the FCC.

3. *Wireless Call Dispatch*

Upon processing the call, the PSAP operator or dispatch center will typically alert the appropriate emergency response team through a wireless land mobile radio system as is indicated by the Number 3 on the figure. During the emergency, these radio systems can be used by emergency units and officers at the scene to coordinate activities amongst themselves, with those units still on their way and with dispatchers and command bases. The FCC regulates the frequencies that these radio systems use, but the systems themselves are customer premises equipment sold directly to the local community by a vendor or vendors. Thus, it is the responsibility of the state and local entities using these wireless systems to inventory them for Y2K related problems and to remediate those problems that are found.

4. *The Emergency Alert System*

The Emergency Alert System (EAS), designated by the Number 4 on the figure, is also an important element of emergency communications. EAS is a national emergency communications system designed to give governments the ability to rapidly communicate with the entire population in times of national emergency.

THE FCC's EMERGENCY SERVICE EFFORTS

The FCC takes responsibility, for its part, to ensure that the Year 2000 challenge vis-a-vis emergency communications is properly addressed. However, inasmuch as the FCC plays an important role by providing information and guidance to companies and critical users (including state and local authorities), encouraging companies to share information, and facilitating the development of readiness and contingency plans, the Commission's ability to address the Year 2000 Problem is not without limits. Only private communications firms and consumers themselves have the ability to address properly the Year 2000 Problem.

For our part, for example, I convened the FCC's very first public forum on Y2K, on the issue of emergency services, in June 1998. Following on the heels of that forum, I felt compelled to promote further this and other important issues, by authoring Y2K awareness articles in as many periodicals as possible. So since the summer 1998, I have authored pieces for the trade magazines of the International Association of Fire Chiefs and the Association of Public Safety Communications Officials-International Inc., as well as a healthy number of telecommunications-related and general media periodicals. I have raised the Y2K issue, in this country and abroad, in numerous speeches. In fact, last week, I addressed the membership of the National Association of Broadcasters at a Y2K Super Session. In addition, FCC Staff members have reached out to numerous members of the public safety community to raise awareness and advocate action on Y2K. A compilation of our efforts to date is appended hereto as Attachment 1.

The FCC has also dedicated much of its Year 2000 efforts to monitoring and assessment of the communications industry's readiness activities including emergency communications. Through surveys, forums, meetings with the industry, information sharing with industry associations and public sources, such as congressional testimony by industry members, the FCC has been monitoring the industries' efforts to the Y2K challenge. In June and July 1998, the FCC organized several roundtables with representatives of different sectors of the communications industry to facilitate information sharing.

A tremendously important contributor to this effort has been the Network Reliability and Interoperability Council (NRIC) which has advised the FCC on the status of the various communications industries' readiness. As you know, much of the information and data that is available to the public, even for areas of concern that are well beyond the FCC's regulatory purview such as foreign telecommunications providers and public safety communications, has been compiled by NRIC. To cite a specific example of this valuable partnership, on March 30, 1999, the FCC in conjunction with NRIC issued its comprehensive Report on the Y2K-readiness. These data and other are continually refreshed as the FCC and NRIC develop a much fuller and well-developed understanding of the efforts of industry sub-sectors.

With fewer than 246 days to January 1, 2000, we continue to develop strategies and approaches to raise industry awareness, to assess and monitor the industries' efforts, and to facilitate the development of effective contingency plans in the event that a disruption to any segment of the communications industry should occur. We will never lose sight of that mission.

ASSESSMENT OF 911 CALL DELIVERY

As previously noted, the FCC issued its comprehensive Y2K Communications Sector Report in March 1999. In our analysis, it was indicated that large local telephone carriers—accounting for 92 percent of the total local telephone lines in the

United States—had achieved 85 percent readiness of their central office switches as of January 1999. These major U.S. carriers are expected to be 100 percent ready by the second quarter of 1999. For their part, small to medium-size carriers lag behind the readiness of their large counterparts and, on average, expect to achieve Y2K-readiness in the fourth quarter of 1999.

These are particularly important statistics because 911 service is provisioned over the public switched telephone network. In brief, 911 calls are routed from the caller to the PSAP by the telecommunication network's 911 tandem switch. The 911 tandem switch is a part of the telephone company's network and is remediated, as required, as part of the telephone company's total Y2K-readiness effort. As a consequence, the readiness of 911 service is, according to the companies, on the same track as the rest of their remediation efforts.

The Telco Year 2000 Forum, the Alliance for Telecommunications Industry Solutions (ATIS), and the Cellular Telecommunications Industry Association (CTIA) have engaged in testing of remediated telecommunications equipment, including 911 testing. In March 1999, the Telco Year 2000 Forum released the results of 1,914 tests and identified only 6 anomalies, none of which affected call processing. The Telco Year 2000 Forum tested 911 emergency call origination as part of four "clusters" of tests of remediated equipment and found no anomalies. On April 14, 1999, ATIS released the results of its efforts on inter-carrier interoperability testing, during which no Year 2000 problems were reported. Finally, also in April 1999, CTIA released the results of its testing efforts, which focused on wireless-to-wireless and wireless-to-wireline, including 911 PSAP calls. In over 825 tests of equipment that that been assessed and remediated, if appropriate, no anomalies relating to the date change were reported.

ASSESSMENT OF CALL PROCESSING AT THE PSAP

PSAP equipment is not telecommunications equipment either under the direct jurisdiction of the FCC or within our area of expertise. We recognize, however, that emergency communications are essential elements at the front and back end of the process. Therefore, we have made every effort to raise awareness in this community of the potential dangers posed by Y2K.

The assessment of the readiness of PSAPs is difficult in general due to the disaggragated nature of the control and ownership of this equipment. We recognize, however, that many telephone companies do have a contractual relationship within their area of service with PSAP owners, most commonly in the form of service and maintenance agreements. As a result, NRIC has made the study of PSAPs through these relationships one of its key study areas within Focus Group 2, the group that concentrates on customer premises equipment.

The NRIC assessment was limited to the 8 largest telephone companies who were asked to estimate the number of PSAPs in their service area, the number of those for which there were service or maintenance agreements with the telephone company, and the number of those for which remediation was complete. On April 14, 1999, NRIC estimated that there were over 7,000 PSAPs total and that the 8 largest telephone carriers had some type of a service contract with 80 percent of the PSAPs in their territory. Of those, NRIC reported, only 10 percent had been remediated. NRIC went on to recommend advising the public to have available the local emergency telephone numbers for police, fire, hospitals, and other emergency services in the event that the PSAPs experience difficulties and the public needs to contact emergency services directly.

Since the time of the release of the NRIC Report, which was based on data gathered in February 1999, there has been an improvement in the number of PSAPs remediated within the service areas of the 8 largest telephone carriers. According to recent reports from the telephone companies, NRIC now estimates that there are a total of 6,739 PSAPs in the territory of the 8 largest telephone companies, and that the companies have service contracts with 81 percent of those, or 5,456 PSAPs. Of that, 5,456, 35 percent of the PSAPs have now been remediated for 911 call processing. The telephone companies also report that they have contacted the remaining PSAPs in their areas with whom they have existing contracts and the they have either begun work or are waiting for the work to be initiated by the PSAP owner.

While these numbers are encouraging, they do not take into account several important factors. First, the new numbers represent only 81% of the PSAPs within the territory of the 8 largest local telephone companies. Further, they do not account for the numerous PSAPs served by the over 1,200 small telephone companies around the country. Second, this assessment is only of PSAPs that have had 911 call processing remediation. It does not necessarily reflect efforts to remediate the wireless call dispatch side of the PSAP process, or other processes the computer may provide for a particular jurisdiction. And while the telephone companies bring expertise and experience to the problem, they too do not have any direct control over the

PSAP and therefore cannot necessarily foresee all the ways in which Y2K may have an impact on the equipment.

We also recognize that the numbers released by NRIC are not consistent with other data released on the overall number of PSAPs. I would stress that the NRIC numbers are only the companies' best estimate of the number of PSAPs in their footprint. The differences, however, only serve to point out the difficulties encountered in trying to get a handle on this issue.

ASSESSMENT OF WIRELESS CALL DISPATCH

Although the FCC has no direct control over the wireless telecommunications equipment used by various emergency response teams, we have made a concerted effort to identify where problems with this equipment may exist and to raise awareness of the need of each service provider to check their own equipment.

Manufacturers report that analog and digital radio systems operating in unencrypted, conventional mode (non-trunked mode not involving computer switching) are not date-sensitive and therefore are not typically at direct risk for Y2K failure. According to data obtained by the Public Safety Wireless Network (PSWN), these systems are the kind operated by the vast majority of state and local public safety agencies, including nearly all smaller and rural agencies. For radios systems using computerized trunking, encryption, gateway and other advanced computerized features that are at higher risk for Y2K failure, manufacturers report that they are engaged in active user notification and remediation assistance programs. The major manufacturers controlling 90 to 95 percent of the public safety equipment market have reported that all new equipment now being sold is Y2K ready, and upgrades or remediation packages for all legacy equipment is now or will shortly be available.

Certain advanced dispatch services such as computer assisted dispatch (CAD) may be at greater risk for Y2K failure, and we understand that replacing these complicated and expensive systems may take more than one year. This means that CAD systems identified now as non-compliant might not be able to be replaced before the year 2000. We understand from the industry, however, that failure of one of these systems, however, should not prevent manual, non-computer assisted emergency dispatch activities until the problem can be solved or a replacement CAD system obtained.

THE EMERGENCY ALERT SYSTEM

The Emergency Alert System (EAS) is also an important element of emergency communications. EAS is a national emergency communications system designed to give governments the ability to rapidly communicate with the entire population in times of national emergency. All broadcast stations and cable systems must participate in EAS; other communications providers may participate voluntarily.

While the EAS system has never been used on a national basis, it is used frequently on a state and local level in times of severe weather or other localized emergency. EAS is structured so that messages can be injected into the system to alert the public. Industry volunteers work to develop EAS plans that use industry facilities in a coordinated, efficient and timely manner. For example, the National Weather Service digital signaling technique used on NOAA Weather Radio and the EAS digital signaling technique are identical.

The EAS system only recently replaced the Emergency Broadcast System, and new equipment capable of receiving and decoding the EAS header codes and emergency messages was required to be installed at broadcast stations by January 1, 1997. Accordingly, virtually all EAS equipment is new and, according to statements by EAS hardware and software manufacturers, both the equipment and software is either compliant or if not compliant, is being updated and provided to customers. Participants at the Commission's Emergency Preparedness Forum confirmed these statements and the overall readiness of the EAS System. Nevertheless, participants did recommend that stations and systems take steps to ensure that they are staffed the night and the morning of December 31, 1999/January 1, 2000.

CONCLUSION

Successful emergency service operations require the coordination and function of many different technical systems and organizations. None can afford not to be Y2K-remediated. As such, with so relatively few days left until January 1, 2000, it is tremendously important that we collectively bring to bear the unique strengths and powers of Congress, the Administration, State and local governments, the Federal Emergency Management Agency, the U.S. Fire Administration, the Department of Justice, the FCC and all other interested stakeholders to address this critical issue.

For the FCCs part, while the direct measures to address Y2K vis-a-vis emergency communications frequently reach well beyond the agency's communications jurisdiction, we do not treat it as though "it's someone else's problem." Indeed, Henry Kissinger once remarked, "competing pressures tempt one to believe that an issue deferred is a problem avoided: more often it is a crisis invited." We at the FCC look

forward to contributing in whatever meaningful form to move public safety organizations towards meeting the Y2K challenge and averting any potential crisis.

Attachment 1: Compilation of FCC Efforts Related to Emergency Communications

	Documents
Aug 1998	Article by Commissioner Powell, *The Year 2000 Bug and Public Safety Communications*, On Scene (trade publication for the International Association of Fire Chiefs).
Apr 1998	Letter from Cable Services Bureau regarding Y2K and EAS
May 29, 1998	Letter from Chairman Kennard and Commissioner Powell to Regional Planning Chairs concerning Y2K, covering emergency communications.
Mar 31, 1999	Y2K Communications Sector Report (with information on emergency communications)
May 1999	Planned release of consumer tips that includes recommendations related to emergency communications.
Ongoing	Maintain FCC Y2K website dedicated to emergency communications information.
	Rulemakings
Sep 29, 1998	The Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, Dkt No.: WT-96-86, FCC No. 98-191, 1st R&O & 3rd NPRM, Para 202-07 (September 29, 1998) (seeking comments, in part, on how the public safety community is addressing the Year 2000 problem).
	Forums & Meetings
Jun 1, 1998	Forum: Public Safety and the Y2K Problem
Jun 12, 1998	Forum: Year 2000 Computer Date Change Issues Affecting the Private Wireless Community
Jun 29, 1998	Forum: Wireline Telecommunications Networks and the Year 2000 Problem
Jun 1998	Meeting: National Association of Broadcasters representatives and the Mass Media Bureau concerning the readiness of EAS equipment.
Jul 16, 1998	Forum: Cable Industry and the Year 2000 Problem
Jul 23, 1998	Forum: Mass Media Bureau's Forum for Broadcasters
Oct 14, 1998	Meeting: Initial meeting of NRIC planning assessment and testing related to 911 and PSAPs.
Nov 10, 1998	Forum: Maintaining Customer Premise Equipment and Private Networks.
Nov 16, 1998	Forum: Y2K Emergency Response Forum
Jan 14, 1999	Meeting: NRIC presentation of preliminary information on assessment and testing related to 911 and PSAPs
Apr 14, 1999	Meeting: NRIC presentation of assessment and testing related to 911 and PSAPs
May 7, 1999	Meeting: Local and State Government Advisory Committee Meeting with Y2K as agenda item – Y2K and emergency services will be primary area of discussion.
	Speeches & Presentations (by John Clark, Deputy Chief, Public Safety and Private Wireless Division, except where noted)
Apr 30, 1998	Congressional Fire Services Institute, Washington, D.C.
May 7, 1998	Denver Interoperability Forum, Denver, Colorado.
May 18, 1998	APCO East Coast Regional Conference, Virginia Beach, Virginia.
May 19, 1998	Federal Wireless Users Forum, Bethesda, Maryland.
Jun 9, 1998	Public Safety Wireless Network Shared Systems Symposium, Boston, Massachusetts.
Jun 13, 1998	Major City (Police) Chiefs Annual Meeting, Sun Valley, Idaho.
Jul 13, 1998	Forestry Conservation Communications Association Annual Meeting, Annapolis, Maryland.
Aug 10, 1998	Regulatory Panel, APCO Annual Conference, Albuquerque, New Mexico.
Aug 11, 1998	Y2K Panel, APCO Annual Conference, Albuquerque, New Mexico.
Aug 12, 1998	Radio Club of America, Annual Breakfast, Albuquerque, New Mexico.
	Documents
Aug 13, 1998	Meet the FCC Presentation, APCO Annual Conference, Albuquerque, New Mexico.
Sep 24, 1998	Public Safety Wireless Network, Chicago Illinois.
Dec 1998	Cable Services Bureau, Western Cable Show.
Mar 15, 1999	APCO Western Regional Conference, San Diego, California.
May 20, 1999	APCO Y2K Symposium.

RESPONSES OF MICHAEL K. POWELL TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Commissioner Powell, it seems as the telephone carriers have done a good job of trying to reach out and prompt the PSAPs to make the necessary phone upgrades. However, even if the PSAPs customer premise equipment is fixed couldn't there still be problems with the other information systems that interface and distribute calls to the emergency responders?

Answer. Yes. The "other information systems that interface and distribute calls to the emergency responders" consist, we are informed, of internal routing systems, computer assisted dispatch ("CAD") systems and land mobile radio systems transmitting both voice and data. Because of the vast number of PSAPs across the country, each with a different mix of equipment elements, it is impossible to predict with any level of specific certainty all the theoretically possible modes of PSAP Y2K failure.

Analog and digital land mobile radio systems of the kind operated by the vast majority of state and local public safety agencies are not date-sensitive and therefore are not typically at direct risk for Y2K malfunction. Radio systems that use trunking and other advanced computerized features are at higher risk for Y2K malfunction. However, manufacturers report that the Y2K vulnerabilities of most of this kind of equipment are well documented, and upgrades and remediation packages are available to agencies that have the resources to acquire them.

Often these expensive systems cannot be remediated cost-effectively and must be replaced. Reversion to manual record keeping and dispatching, though slower and inefficient, is an available contingency method if a PSAP system fails. Internal routing systems also are of many different varieties and may or may not rely on computers that are susceptible to the Y2K Problem.

The most vexing problem confronting even those PSAPs that have been diligent about Y2K preparation is that even though their individual equipment elements test as Y2K-ready, the interaction of all the elements together cannot be certified because the whole system is in operation twenty-four hours per day and cannot be safely taken offline to be tested.

Question 2. In August, you published an article in a public safety communication magazine published by the International Associations of the Chiefs of Police. Did you or the FCC get a sense that the law enforcement community understood the risks they were facing from Y2K?

Answer. It is difficult for us to say. Although the Federal Communications Commission licenses the radio systems in the possession of tens of thousands of state and local law enforcement agencies across the country, the agency is not the best situated to observe or describe the sate of understanding in the law enforcement community as a whole regarding the complicated Y2K issue. That being said, the Commission, along with other federal agencies like the Federal Emergency Management Agency and the Departments of Justice and Treasury, and organizations like the Association of Public Safety Communications Officers, International, the International Association of Chiefs of Police and the International Association of Fire Chiefs, have made significant efforts in the past sixteen months to alert the public safety community to the serious risks of the Y2K Problem.

Many agencies, to their credit, have also responded to this important technical problem. For example, the Federal Bureau of Investigation, inaugurated its NCIC 2000 system last Sunday, July 11, 1999. On July 28, 1999, that agency will begin operating its Integrated Automatic Fingerprint Identification System ("IAFIS"). Both systems provide nationwide electronic access to criminal record information for law enforcement. Every state has become qualified to participate in both systems, where qualification included a certification of Y2K readiness for each state's law enforcement computer system.

Overall, the evaluations of Y2K awareness proffered by members of the law enforcement community indicate that most of the law enforcement agencies at the state level and in the larger metropolitan counties and cities, with larger budgets and technical staffs, are generally well aware of the Y2K Problem. Although progress is by no means uniform, many have designed or implemented Y2K remediation plans, contingency plans for their agencies and their jurisdictions, and are, or will be prepared for the millennial date rollover. We are told that it is likely, however, that many more smaller, more rural and more resource-strapped agencies, despite the best efforts of many to reach them, are as yet still unaware of, unwilling or unable to address this problem.

Question 3. You mentioned that the Public Safety Wireless Safety Network feels that small and rural radio systems are typically analog and as a result are less vul-

nerable to direct Y2K failure. Would it be safe to say that the fast growing counties and rapidly modernizing communities are at an increased risk from Y2K?

Answer. In 1998 and 1999, the Public Safety Wireless Network conducted a survey of 3,398 of the more than 36,000 state and local fire and emergency medical agencies in the U.S. and found that 75% operated conventional, not trunked, radio systems. Approximately 90% of fire and EMS agencies with fewer than 50 personnel operated conventional mode radio systems. Because the majority of emergency service organizations do not rely on computerized switching or trunking, these systems, including both analog and digital systems, we are told by the industry that these systems are generally at low risk for Y2K malfunction.

The same Public Safety Wireless Network survey found that nearly 40% of fire and EMS agencies with more than 250 personnel employ trunked radio systems. These statistics support the theory that the public safety agencies in larger cities and counties and those that have upgraded their communications equipment to employ the most advanced features are at relatively heightened risk for Y2K malfunction of the date-sensitive computers and electronic components that provide those features.

Question 4. How successful was the September 98 rulemaking on the development of operational and technical spectrum through 2010? Do you feel it has been successful in getting the wireless community to take Y2K seriously?

Answer. Our actions in the September 1998 First Report and Order and Third Notice of Proposed Rulemaking, WT Docket No. 96–86, *The Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010 Establishment of Rules and Requirements For Priority Access Service ("First Report")*, took significant steps toward resolving certain of the telecommunications challenges facing the public safety community, including, but not limited to, making available sufficient spectrum to take advantage of innovation in technology.

Specifically, in the *First Report*, the Commission concluded that it is important to increase our efforts to alert the public safety communications community to the nature and seriousness of the Year 2000 problem and to ascertain both the current state of Y2K readiness and the progress and range of compliance initiatives in that community. The Commission sought comment on how best to ascertain the extent, reach, and effectiveness of Year 2000 compliance initiatives that have been or are being undertaken by public safety entities, so that we can better understand the nature of the Year 2000 problem and the potential risks posed to public safety communications networks.

I believe that the Commission was successful in raising the awareness of the Year 2000 Problem. For instance, nine of 23 formal commenters and three of 14 reply commenters addressed the Y2K issues for which we sought comment. The commenters include, the Association of Public-Safety Communications Officials-International, Inc. ("APCO"), the Federal Law Enforcement Wireless Users Group ("FLEWUG"), the International Association of Chiefs of Police ("IACP"), Joint Comments of American Association of State Highway and Transportation Officials ("AASHTO"), Forestry Conservation Communications Association ("FCCA"), International Association of Fire Chiefs ("IAFC"), International Association of Fish and Wildlife Agencies ("IAFWA"), International Municipal Signal Association ("IMSA") and National Association of State Foresters ("NASF") (collectively, "Joint Commenters"), National Public Safety Telecommunications Council ("NPSTC"), Public Safety Wireless Network Program ("PSWN"), Motorola, Inc., the State of California, the State of Florida, and the National League of Cities and the City of San Francisco.

These aforementioned commenters represent a significant cross-section of the public safety wireless community and stated that they view the Y2K Problem as an important issue that can affect their operations. They generally stated that the Commission should continue its outreach effort and offered to assist the Commission to inform the community regarding the Y2K Problem. As an example, APCO, which reaches a majority of public safety users through its frequency coordination efforts, held a national Y2K symposium in Illinois on May 20–21, 1999 in an effort to further educate users. FCC staff attended and summarized information the commenters provided in WT Docket No. 96–86 regarding the Y2K matters, as well as summarized the FCC/Network Reliability and Interoperability Council's joint document "Y2K Communications Sector Report."

○